Calculs dans les jacobiennes de courbes algébriques, applications en géométrie algébrique réelle.

Valéry Mahé

N° d'Ordre : 3327

THÈSE

Présentée

DEVANT L'UNIVERSITÉ DE RENNES 1

pour obtenir

le grade de DOCTEUR DE L'UNIVERSITÉ DE RENNES 1

Mention Mathématiques et Applications

par

Valéry MAHÉ

Institut de Recherche Mathématique de Rennes

École Doctorale MATISSE

U.F.R. de Mathématiques

TITRE DE LA THÈSE

Calculs dans les jacobiennes de courbes algébriques, applications en géométrie algébrique réelle

Soutenue le 28 septembre 2006 devant la Commission d'Examen

Composition du jury

M. J.-M. COUVEIGNES	Examinateur
M. J. van GEEL	Rapporteur
M. J. HUISMAN	Examinateur
M. R. LERCIER	Examinateur
M. D. LUBICZ	Directeur de thèse
M. L. MAHÉ	Directeur de thèse
M. P. SATGÉ	Rapporteur

Table des matières

Remerciements

Je veux tout d'abord remercier chaleureusement mes deux directeurs de thèse : David Lubicz et Louis Mahé. Sans leur soutien et leurs conseils avisés cette thèse n'aurait jamais pu aboutir.

Lors de mon stage de DEA, David Lubicz m'a fait découvrir la notion de jacobienne. Au cours de ma thèse ses conseils m'ont été très précieux. Malgré l'éloignement géographique, il a toujours trouvé le temps pour m'aider et n'a pour cela jamais hésité à se déplacer. Je l'en remercie.

Pendant toutes ces années, Louis Mahé m'a toujours accueilli dans son bureau avec le sourire. Sa passion pour les mathématiques est communicative, et je me souviendrai toujours avec plaisir de toutes ces heures de discussions mathématiques. Je veux donc le remercier pour sa gentillesse et sa très grande disponibilité.

Malgré la date à laquelle je leur ai fourni le premier exemplaire, Jan van Geel et Philippe Satgé m'ont fait l'honneur d'être les rapporteurs de cette thèse. Ils ont aussi accepté d'être membres de mon jury de thèse. Je leur en suis extrêmement reconnaissant.

Je tiens aussi à remercier chaleureusement Jean-Marc Couveignes, Johannes Huisman et Reynald Lercier d'avoir accepté de faire partie de mon jury de thèse.

Pendant toutes ces années j'ai pris plaisir à travailler à l'IRMAR et en particulier au contact des équipes de "géométrie algébrique" et de "géométrie algébrique réelle et calcul formel" dont les membres ont toujours été sympathiques et prêts à m'aider. Mes excellentes conditions de travail tiennent aussi à l'efficacité des personnels administratifs de l'IRMAR. Un grand merci à tous.

Je veux également exprimer ma gratitude envers tous ceux qui, par leurs enseignements à l'université ou à l'antenne de bretagne de l'ENS Cachan, m'ont aidé à développer mon goût pour les mathématiques.

Pendant trois ans, j'ai partagé le même bureau que Sylvain. Durant tout ce temps (et particulièrement l'été 2005) son soutien et son amitié m'ont été indispensables. Je ne peux le remercier sans exprimer ma gratitude envers

Fanny, à qui j'envoie tous mes encouragements pour l'année qui vient.

L'amitié de Karel m'a été tout aussi précieuse. Sans son soutien (et radio Hitalia) je n'aurais jamais eu le courage de terminer cette thèse. Je le remercie aussi pour m'avoir accompagné pendant toutes ces longues soirées et ces longs week-ends de travail.

Je souhaite aussi remercier Adeline pour m'avoir soutenu depuis la Lorraine. Son dynamisme et sa joie de vivre m'ont remonté la moral lorsque j'en avais besoin.

J'ai eu la chance de partager mon bureau avec de nombreuses personnes fort sympathiques : Frédéric, Thomas (merci à tous les deux pour les discussions linuxiennes), Amaury (ton expérience m'a été précieuse), Gweltaz (un grand merci pour le foot), Pierre (toutes ces soirées passées à camper), Gwenael, Colas, Daniel et Viviana. Je dois leur associer aussi Jérome et Christian qui ont participé à la vie du bureau 620, bien que n'en faisant pas officiellement partie. Je vous remercie tous pour votre gentillesse.

Sandrine était là à chaque fois que je me posais des questions administratives. Je la remercie pour son aide et sa patience.

Je remercie aussi les membres du groupe des "mange-tôt", les participants du séminaire "pampers", les "footeux" du vendredi soir et plus généralement tous les doctorants de l'IRMAR. Ils m'ont tous aidés à me sentir bien au sein de l'IRMAR.

J'ai aussi une pensée pour ma famille et mes amis : je sais que je n'ai pas été aussi présent et facile à vivre que je ne l'aurais souhaité. Je vous remercie tous de m'avoir soutenu malgré tout pendant cette thèse. Enfin je souhaite remercier mon institutrice de CP (mademoiselle Botcazou) pour m'avoir appris à aimer les mathématiques.

Introduction

Attention :

Lorsque nous faisons référence au nom de Mahé, nous parlons de Louis Mahé, qui est un homonyme de l'auteur, mais n'est pas de la même famille que lui (le nom de famille Mahé est l'un des plus courant en bretagne).

Soit $P \in \mathbb{R}[X_1, \cdots, X_n]$ un polynôme. Si P est une somme de carrés dans $\mathbb{R}(X_1, \cdots, X_n)$, alors P est positif ou nul sur $\mathbb{R}^n$ (i.e. $\forall (x_1, \cdots, x_n) \in \mathbb{R}^n, P(x_1, \cdots, x_n) \geq 0$). Réciproquement, lorsque P est positif ou nul sur $\mathbb{R}^n$, nous pouvons nous demander si P est une somme de carrés de fractions rationnelles. Cette question est connue sous le nom de dix-septième problème de Hilbert. En 1927 Artin apporte une réponse positive avec le théorème (voir [Art27]) :

Théorème 1 (Artin) *Soient R un corps réel clos et $f \in R[X_1, \cdots, X_n]$. Si f est positif ou nul sur R^n, alors f est somme de carrés dans le corps des fractions rationnelles $R(X_1, \cdots, X_n)$.*

Une question connexe est l'aspect quantitatif : il s'agit de déterminer le nombre minimum r tel que tout polynôme positif puisse s'écrire comme une somme de r carrés de fractions rationnelles. La réponse à cette question n'est pas complètement connue. À ce sujet, Hilbert montre que les polynômes en deux variables positifs ou nuls sur $\mathbb{R}^2$ sont somme de quatre fractions rationnelles. Il montre également que les polynômes en deux variables de degré total inférieur à 4 sont somme de trois carrés de polynômes. Le premier de ces deux résultats est généralisé par Pfister de la manière suivante : tout élément de $\mathbb{R}[X_1, \cdots, X_n]$ positif ou nul sur $\mathbb{R}^n$ peut s'écrire comme une somme de 2^n carrés de fractions rationnelles.

On ne dispose pas d'une caractérisation effective des sommes de trois carrés dans $\mathbb{R}(X, Y)$. Cependant, en 1971, Cassels, Ellison et Pfister donnent un premier exemple de polynôme positif qui n'est pas somme de trois carrés de fractions rationnelles (voir [CEP71]) :

Théorème 2 (Cassels, Ellison et Pfister) *Le polynôme de Motzkin $M(X, Y) = 1 + X^2Y^4 + X^4Y^2 - 3X^2Y^2$ est positif ou nul sur $\mathbb{R}^2$ (et donc*

somme de quatre carrés de fractions rationnelles) mais n'est pas somme de trois carrés dans $\mathbb{R}(X,Y)$.

Pour démontrer ce théorème, Cassels, Ellison et Pfister associent à tout polynôme positif de la forme $F(X,Y) = 1 + A(X)Y^2 + B(X)Y^4 \in \mathbb{R}(X,Y)$ avec $B(A^2 - 4B) \neq 0$ la courbe elliptique $\mathcal{E}_F$ d'équation affine

$$-\beta^2 = \alpha(\alpha^2 - 2A(x)\alpha + A(x)^2 - 4B(x)).$$

Ils expliquent alors que F est somme de trois carrés dans le corps $\mathbb{R}(X,Y)$ si et seulement si $\mathcal{E}_F$ possède un $\mathbb{R}(x)$-point (α,β) tel que α et $-(\alpha^2 - 2A(x)\alpha + A(x)^2 - 4B(x))$ soient des sommes de deux carrés dans $\mathbb{R}(x)$ (c'est-à-dire positifs ou nuls sur $\mathbb{R}$). Une méthode similaire permet à Christie d'exhiber (dans [Chr76]) une famille de polynômes positifs ou nuls sur $\mathbb{R}^2$ qui ne sont pas somme de trois carrés de fractions rationnelles :

Théorème 3 (Christie) *Soient* λ, μ, ν *trois entiers tels que* $0 < \mu < \nu$, $\mu = (-3)^n\lambda$ *pour* $n \in \mathbb{N}^*$ *et* λ *non multiple de* 3 *vérifiant* $\lambda \equiv -\nu[3]$. *Nous supposons que* $3\mu(\mu-\nu)$ *et* $\mu^2 + \mu\nu + \nu^2$ *ne sont pas des carrés d'entiers.*

Alors le polynôme $1 + X((X+\mu)^3 - \frac{\nu^3}{2})Y^2 + \frac{1}{16}\nu^6X^2Y^4$ *est défini positif mais n'est pas somme de* 3 *carrés dans* $\mathbb{R}(X,Y)$.

Utilisant une stratégie totalement différente (basée sur le théorème de Noether-Lefschetz), Colliot-Thélène prouve en 1992 le théorème (voir [CT93]) :

Théorème 4 (Colliot-Thélène) *Soient* $m \geq 3$ *un entier et* $N = \frac{(m+2)(m+1)}{2}$. *Soient* $l(T_1,\cdots,T_N) = \sum_{1\leq i\leq N} a_iT_i$ *une forme linéaire à coefficients dans* $\mathbb{R}$ *et* $q(T_1,\cdots,T_N) = \sum_{1\leq i\leq j\leq N} b_{i,j}T_iT_j$ *une forme quadratique à coefficients dans* $\mathbb{R}$. *Si nous nous donnons un ordre sur l'ensemble des couples d'entiers naturels* (a,b) *avec* $a+b \leq m$, *nous pouvons définir un morphisme*

$$\begin{array}{rccc} \varphi : & \mathbb{A}^2 & \longrightarrow & \mathbb{A}^N. \\ & (X,Y) & \longmapsto & (X^aY^b) \end{array}$$

Nous posons alors $P(X,Y) := (4q - l^2)(\varphi(X,Y))$.

1. *Si les coefficients* $(a_i)_{1\leq i\leq N}$ *et* $(b_{i,j})_{1\leq i\leq j\leq N}$ *sont algébriquement indépendants sur* $\mathbb{Q}$, *alors le polynôme* $P(X,Y)$ *n'est pas somme de trois carrés dans* $\mathbb{R}(X,Y)$.
2. *Il existe un nombre réel* $\epsilon > 0$ *tel que si les coefficients* $(a_i)_{1\leq i\leq N}$ *et* $(b_{i,j})_{1\leq i\leq j\leq N}$ *vérifient les inégalités* $|a_i| < \epsilon$, $|b_{i,i} - 1| < \epsilon$ *et* $|b_{i,j}| < \epsilon$ *pour* $i \neq j$, *alors le polynôme* $P(X,Y)$ *est strictement positif sur* $\mathbb{R}^2$.

Dans [Mac00], Macé utilise la méthode développée par Cassels, Ellison et Pfister pour étudier des polynômes de la forme $(Y^2+a(X))(Y^2+b(X))$ avec a, $b \in \mathbb{R}(x)$ des fractions rationnelles positives ou nulles sur $\mathbb{R}$. Il montre notamment :

Théorème 5 (Macé) *Soit $0 < r < 1$ un nombre réel. Alors le polynôme strictement positif $F(X,Y) := (Y^2 + (X^2+1)^2)(Y^2 + (X^2+1)^2 - r^2)$ n'est pas une somme de trois carrés dans $\mathbb{R}(X,Y)$ si les deux conditions suivantes sont vérifiées :*

* *r et $r(r+1)$ ne sont pas des carrés dans le corps $\mathbb{Q}(r)$;*
* *l'un des trois nombres $(1-r)$, $(1+r)$ et 2 n'est pas un carré dans le corps $\mathbb{Q}(r)$.*

Les résultats présentés dans [Mac00] ne font intervenir que des courbes elliptiques de $\mathbb{C}(X)$-rang de Mordell-Weil nul. Certains de ces résultats sont étendus en 2005 par Macé et Mahé dans [MM05] : les courbes elliptiques qu'ils étudient sont de $\mathbb{R}(x)$-rang de Mordell-Weil nul sans être de $\mathbb{C}(x)$-rang de Mordell-Weil nul.

Théorème 6 (Macé, Mahé) *Soit $P(X,Y) := Y^4 + A(X)Y^2 + B(X)$ avec $A(X) := X^4 + \left(\frac{1+3r}{2}\right)X^2 + r^2$ et $4B(X) := X^4\left(X^2 + r - \frac{1}{4}\right)\left(X^2 + 2r - 1\right)$ où $r > \frac{3}{4}$, $r \neq 1$ est un réel tel que $6r(4r-1)$ et $6r(2r-1)$ ne soient pas des carrés dans $\mathbb{Q}(r)$.*

Alors P est une somme de quatre carrés dans $\mathbb{R}(x,y)$ qui n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$.

La méthode développée par Cassels, Ellison et Pfister ne permet d'étudier que des polynômes de la forme $Y^4 + A(X)Y^2 + B(X)$: cette forme est indispensable pour définir la courbe elliptique centrale à leur étude. En 2001, Huisman et Mahé généralisent la construction de Cassels, Ellison et Pfister à l'aide de la notion de point antineutre.

Un $\mathbb{R}(x)$-point P d'une variété abélienne A définie sur $\mathbb{R}(x)$ est dit antineutre si pour toute clôture réelle k de $\mathbb{R}(x)$ le point P n'est pas dans la composante neutre de $A(k)$ Dans [HM01], Huisman et Mahé montrent qu'un polynôme $P(X,Y)$ de degré en Y multiple de 4 est une somme de trois carrés dans le corps $\mathbb{R}(X,Y)$ si et seulement si un $\mathbb{R}(x)$-point de la jacobienne de la $\mathbb{R}(x)$-courbe hyperelliptique $\mathcal{C}$ d'équation affine $z^2 + P(x,y) = 0$ est antineutre.

L'objet cette thèse est de généraliser la méthode de Cassels, Ellison et Pfister à l'aide du résultat de Huisman et Mahé. Nous obtenons en particulier une famille d'éléments de $\mathbb{R}[x,y]$ de degré 8 en y, positifs ou nuls sur $\mathbb{R}^2$, qui ne sont pas somme de trois carrés dans $\mathbb{R}(x,y)$. L'idée générale est de chercher des polynômes $P(x,y)$ tels que le groupe $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ soit de $\mathbb{R}(x)$-rang de Mordell-Weil nul : $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est alors égal à sa torsion et nous n'avons à tester l'antineutralité que d'un nombre fini d'éléments de $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$. Pour montrer la nullité du $\mathbb{R}(x)$-rang de Mordell-Weil de la jacobienne considérée, nous effectuons une 2-descente.

Dans une première partie nous mettons en place tous les outils nécessaires à notre étude ; il s'agit donc principalement d'une partie d'exposition. Nous

commençons ainsi par rappeler les résultats de Huisman et Mahé afin de reformuler correctement notre problème, puis nous expliquons le principe général de l'étude.

Nous poursuivons cette partie par des rappels concernant la notion de représentation de Mumford. Soit $\mathcal{H}$ une courbe hyperelliptique donnée par une équation affine de la forme $z^2 = f(y)$ avec f unitaire, sans facteur carré et de degré impair. Un élément P de $\mathrm{Jac}(\mathcal{H})$ est représenté par un couple (u, v) de polynômes en y, sa représentation de Mumford. Si un point α de $\mathrm{Jac}(\mathcal{H})$ s'écrit $\alpha = j(\alpha_1) + \cdots + j(\alpha_n)$ avec $j : \mathcal{H} \longrightarrow \mathrm{Jac}(\mathcal{H})$ l'injection canonique et α_i un point de $\mathcal{H}$, le polynôme u code les abscisses des α_i et v les ordonnées. La représentation de Mumford ne peut pas être utilisée pour toutes les courbes hyperelliptiques. Cependant, les polynômes $P(x, y)$ positifs ou nuls sur $\mathbb{R}^2$ auxquels nous nous intéressons dans cette thèse sont choisis de la forme $P(x, y) = (y^2 + 1)Q(x, y^2)$ avec $Q(x, y) \in \mathbb{R}[x, y]$. Ainsi, grâce à un changement de variable, la représentation de Mumford permet de manipuler les points de la jacobienne de la courbe hyperelliptique d'équation affine $z^2 + (y^2 + 1)Q(x, y^2) = 0$.

Soit k un corps de caractéristique 0 sur lequel $\mathcal{H}$ est définie. Le premier chapitre se termine par la présentation d'un morphisme dont le noyau est $2\mathrm{Jac}(\mathcal{H})(k)$. Ce morphisme a été introduit par Cassels pour les courbes elliptiques et sa généralisation aux jacobiennes de courbes hyperelliptiques est due à Schaefer. C'est pourquoi nous avons choisi d'appeler ce morphisme le morphisme de Cassels-Schaefer. Cette caractérisation des doubles a deux utilités : non seulement elle simplifie l'étude de la torsion 2-primaire (chapitre 2), mais elle est également centrale lors de la 2-descente (chapitre 3) et des calculs de rangs de Mordell-Weil réalisés au cours des chapitres 3 et 4.

La deuxième partie est consacrée à l'étude des points de torsion 2-primaire pour deux types de courbes hyperelliptiques. Nous fixons un polynôme $Q(x, y) \in \mathbb{R}(x)[y]$ tel que $P(x, y) := (y^2 + 1)Q(x, y^2) \in \mathbb{R}(x)[y]$ soit positif ou nul sur $\mathbb{R}^2$, unitaire, sans facteur carré, et de degré en y multiple de 4 strictement positif. Nous notons $\mathcal{C}$ la courbe hyperelliptique d'équation affine $z^2 + P(x, y) = 0$ et g le genre de $\mathcal{C}$. Nous expliquons tout d'abord comment vérifier qu'un point de $\mathrm{Jac}(\mathcal{C})$ est $\mathbb{R}(x)$-rationnel. Nous signalons aussi qu'un point $\alpha \in \mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ de représentation de Mumford (u, v) est antineutre si et seulement si

* α est $\mathbb{R}(x)$-rationnel,
* u de degré g, et
* $u(0)$ est une somme non nulle de deux carrés dans $\mathbb{R}(x)$ (i.e. une fraction rationnelle en une variable positive ou nulle sur $\mathbb{R}$).

Si nous souhaitons montrer que P est une somme de trois carrés, il est naturel de commencer par chercher un point antineutre parmi les points de torsion. En fait, étudier la torsion 2-primaire suffit : l'existence d'un élément de torsion antineutre de $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est équivalente à l'existence

d'un élément de torsion 2-primaire antineutre de $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$.

Au cours de la section 2.3.1, nous expliquons comment calculer la torsion 2-primaire de $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ en itérant la division par 2.

L'addition dans $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ peut s'effectuer en termes de représentation de Mumford. En écrivant la formule de doublement d'un point, nous obtenons, pour tout point fixé $\alpha \in \mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$, une équation dont les solutions correspondent aux représentations de Mumford des points β tels que $2\beta = \alpha$.

Cependant, cette équation de division par 2 reste assez compliquée. Une raison de cette complexité est que tous les éléments de $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ ne sont pas dans $2\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$. Afin de simplifier la résolution de l'équation de division par 2, nous décidons de faire appel à la caractérisation de Schaefer des éléments de $2\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$.

Nous déterminons finalement les points de torsion antineutres en appliquant la méthode suivante. Nous vérifions d'abord la antineutralité des points de 2-torsion. Lorsque le groupe $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))[2^r]$ des éléments 2^r-torsion de $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ a été calculé nous appliquons à tout point $\alpha \in \mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))[2^r]$ l'algorithme suivant :

1. déterminer si l'image $\pi_{\mathcal{C}}(\alpha)$ de α par le morphisme de Cassels-Schaefer $\pi_{\mathcal{C}}$ (associé à $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$) est triviale ;
2. si l'image $\pi_{\mathcal{C}}(\alpha)$ est triviale, trouver un élément $\beta \in \mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ tel que $2\beta = \alpha$ (en résolvant l'équation de division par 2 associé à α) :
3. Si $\pi_{\mathcal{C}}(\alpha)$, n'est pas triviale, étudier, pour tout $T \in \mathrm{Jac}(\mathcal{C})(k)[2]$, l'antineutralité de $T + \alpha$.

Ce faisant, nous déterminons le groupe $\mathrm{Jac}(\mathcal{C})(k)[2^{r+1}]$ des éléments 2^{r+1}-torsion de $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$. Nous pouvons alors passer à l'étape $r+1$.

Cette procédure est appliquée à deux familles de courbes, mais avec deux optiques différentes. La première famille est obtenue en prenant

$$P(x,y) = (y^2+1)(y^2+C(x^2))(y^4+(1+C(x^2))y^2+B(x^2)$$

avec B, $C \in \mathbb{R}[x]$ des polynômes réels positifs ou nuls sur $\mathbb{R}$ de degrés respectivement 2 et 1 tels que le polynôme $(1+C)^2 - 4B$ soit de degré 1. Cette famille est destinée à fournir des exemples d'élément de $\mathbb{R}(x)[y]$ de degré 8 positifs ou nuls sur $\mathbb{R}^2$ qui ne sont pas somme de trois carrés dans $\mathbb{R}(x,y)$. Dans la section 2.4, nous énonçons des conditions de généricité sur les coefficients B et C assurant que la torsion 2-primaire du groupe $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ est engendrée par un élément de 8-torsion et un élément de 2-torsion. Nous en déduisons ensuite que $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ n'a aucun élément de torsion antineutre.

Dans la section 2.5 , nous étudions des polynômes de la forme

$$P(x,y) = (y^2+1)(y^2+a)(y^2+b)(y^2+c)$$

avec a, b, $c \in \mathbb{R}(x)$. Le point de vue que nous adoptons est l'opposé du précédent : il s'agit ici de trouver des conditions sur les coefficients a, b et c

sous lesquelles le polynôme $(y^2+1)(y^2+a)(y^2+b)(y^2+c)$ est somme de trois carrés dans $\mathbb{R}(x,y)$. Pour cela, nous calculons la 2-torsion et la 4-torsion de $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$, puis nous cherchons à savoir si l'un des points ainsi trouvés est un $\mathbb{R}(x)$-point antineutre. Nous aboutissons finalement au théorème

Théorème 7 *Soient α, β, et $\gamma \in \mathbb{R}(x)$ trois fractions rationnelles non nulles. Nous supposons que β^2 est différent de γ^2. Nous posons*

$$\begin{array}{l} a = 1+\alpha^2(1+\beta^2)(1+\gamma^2), \\ b = 1+\alpha^2(1+\beta^2)^2(1+\gamma^2) \text{ et} \\ c = 1+\alpha^2(1+\beta^2)(1+\gamma^2)^2. \end{array}$$

Alors le polynôme $P(y) := (y^2+1)(y^2+a)(y^2+b)(y^2+c)$ est somme de trois carrés dans $\mathbb{R}(x,y)$:

$$\begin{aligned} P(y) \;=\; & \Big(-\tfrac{(a-1)y(y^2+a)}{\alpha} + \alpha\beta\gamma((1-\beta\gamma)y+\beta+\gamma)(y^2+1)\Big)^2 \\ & + \Big(-\tfrac{(a-1)(y^2+a)}{\alpha} + \alpha\beta\gamma(1-\beta\gamma-(\beta+\gamma)y)(y^2+1)\Big)^2 \\ & + \big((y^2+1)(y^2+a-\beta\gamma)\big)^2. \end{aligned}$$

Au cours des chapitres 3 et 4, nous donnons une famille de polynômes qui ne sont pas somme de trois carrés dans $\mathbb{R}(x,y)$. Soient η, ω, $\rho \in \mathbb{R}$ des réels et $k := \mathbb{Q}(\eta,\omega,\rho)$. Nous posons :

$$b_1 = \frac{\rho^2-\eta^2}{\omega^2-\eta^2} + \frac{\eta^2-\omega^2}{4}.$$

Soient $B(x) := (x+b_1)^2-\eta^2$ et $C(x) := 2(x+b_1)+\omega^2-\eta^2-1$. Nous notons

$$P(x,y) := (y+1)(y+C(x))(y^2+(1+C(x))y+B(x)).$$

Nous supposons que le polynôme $P(x^2,y^2)$ est sans facteur carré.

Sous certaines conditions de nature arithmétique dans le corps k, nous montrons que le polynôme $P(x^2,y^2)$ n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$. Pour cela, nous considérons la courbe hyperelliptique $\mathcal{C}$ sur $\mathbb{R}(x)$ d'équation affine $z^2+P(x^2,y^2)=0$.

Lors de la section 2.4, nous énonçons des conditions de généricité sur les coefficients B et C sous lesquelles le groupe $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ n'a aucun élément de torsion antineutre. Pour montrer que $P(x^2,y^2)$ n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$, il suffit désormais de prouver que le rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est nul. Dans le troisième chapitre, nous simplifions l'étude du $\mathbb{R}(x)$-rang de Mordell-Weil de la jacobienne $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$.

Nous utilisons tout d'abord la parité en y du polynôme $P(x^2,y^2)$: le rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est la somme des rangs de Mordell-Weil de $\mathrm{Jac}(\mathcal{C}^+)(\mathbb{R}(x))$ et $\mathcal{C}^-(\mathbb{R}(x))$ avec

* $\mathcal{C}^+$ la courbe hyperelliptique de genre 2 d'équation affine $z^2 + yP(x^2, y) = 0$
* et $\mathcal{C}^-$ la courbe elliptique d'équation affine $z^2 + P(x^2, y) = 0$.

Cette simplification est importante pour la suite : montrer directement que le rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est nul engendrerait des calculs trop importants (le genre de la courbe $\mathcal{C}$ est 3).

La parité en x du polynôme $P(x^2, y)$ peut également être exploitée. Pour cela, nous notons, pour tout $\delta \in k(x)$,

* $\mathcal{C}_\delta^+$ la courbe hyperelliptique sur $k(x)$ de genre 2 d'équation affine $\delta z^2 + yP(x, y) = 0$,
* et $\mathcal{C}_\delta^-$ la courbe elliptique sur $k(x)$ d'équation affine $\delta z^2 + P(x, y) = 0$.

Le $\mathbb{R}(x)$-rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})$ est nul si et seulement si $\mathcal{C}_1^-$, $\mathcal{C}_x^-$, $\mathrm{Jac}(\mathcal{C}_1^+)$ et $\mathrm{Jac}(\mathcal{C}_x^+)$ sont de $\mathbb{R}(x)$-rangs de Mordell-Weil nuls.

Au cours des sections 3.3 et 3.4, nous appliquons un lemme de Christie (voir [Chr76]) pour effectuer une 2-descente. Nous montrons ainsi que le $\mathbb{R}(x)$-rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})$ est nul si et seulement si pour tout élément strictement positif ζ de k les $k(x)$-rangs de Mordell-Weil de $\mathcal{C}_\zeta^-$, $\mathcal{C}_{\zeta x}^-$, $\mathrm{Jac}(\mathcal{C}_\zeta^+)$ et $\mathrm{Jac}(\mathcal{C}_{\zeta x}^+)$ sont nuls. La 2-descente est essentielle : le corps $k(x)$ est plus adapté aux calculs de Mordell-Weil que le corps $\mathbb{R}(x)$.

Ici, le choix des coefficients B et C n'est pas anodin : nous ne pouvons effectuer la 2-descente que si les conditions suivantes sont vérifiées :

* les polynômes B, C, $B - C$ et $1 - C$ sont scindés sur k,
* le polynôme $(1 + C(x))^2 - 4B(x)$ est de degré 1 et son évaluation en 0 est un carré dans k.
* les polynômes $B(x^2)$, $C(x^2)$, $B(x^2)C(x^2)$, $B(x^2) - C(x^2)$, $(B(x^2) - C(x^2))(1 - C(x^2))$ et $(1 + C(x^2))^2 - 4B(x^2)$ ne sont pas des carrés dans $\mathbb{C}(x)$
* le polynôme $1 - C$ est premier à x, B, $B - C$ et $(1 + C)^2 - 4B$.

Dans la section 3.5, nous tirons parti de l'existence, pour tout $\delta \in k(x)^\times$, de deux isogénies de Richelot $\varphi^+ : \mathrm{Jac}(\mathcal{C}_\delta^+) \longrightarrow \mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)$ et $\varphi^- : \mathcal{C}_\delta^- \longrightarrow \widehat{\mathcal{C}}_\delta^-$. Ces deux isogénies de Richelot nous permettent de simplifier les calculs de rangs de Mordell-Weil (voir par exemple [CF96]). Ainsi, le $\mathbb{R}(x)$-rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})$ est nul si et seulement si, pour tout $\zeta \in k$ strictement positif, les images de huit homomorphismes

$$\gamma_{\mathcal{C}_\zeta^-},\ \gamma_{\mathcal{C}_{\zeta x}^-},\ \gamma_{\widehat{\mathcal{C}}_\zeta^-},\ \gamma_{\widehat{\mathcal{C}}_{\zeta x}^-},\ \Pi_{\mathcal{C}_\zeta^+},\ \Pi_{\mathcal{C}_{\zeta x}^+},\ \Pi_{\widehat{\mathcal{C}}_\zeta^+} \text{ et } \Pi_{\widehat{\mathcal{C}}_{\zeta x}^+}$$

sont respectivement les images des points de torsion $k(x)$-rationnels de

$$\mathcal{C}_\zeta^-,\ \mathcal{C}_{\zeta x}^-,\ \widehat{\mathcal{C}}_\zeta^-,\ \widehat{\mathcal{C}}_{\zeta x}^-,\ \mathrm{Jac}(\mathcal{C}_\zeta^+),\ \mathrm{Jac}(\mathcal{C}_{\zeta x}^+),\ \mathrm{Jac}(\widehat{\mathcal{C}}_\zeta^+) \text{ et } \mathrm{Jac}(\widehat{\mathcal{C}}_{\zeta x}^+).$$

Le quatrième chapitre est consacré à l'étude des images de $\gamma_{\mathcal{C}_\zeta^-}$, $\gamma_{\mathcal{C}_{\zeta x}^-}$, $\gamma_{\widehat{\mathcal{C}}_\zeta^-}$, $\gamma_{\widehat{\mathcal{C}}_{\zeta x}^-}$, $\Pi_{\mathcal{C}_\zeta^+}$, $\Pi_{\mathcal{C}_{\zeta x}^+}$, $\Pi_{\widehat{\mathcal{C}}_\zeta^+}$ et $\Pi_{\widehat{\mathcal{C}}_{\zeta x}^+}$. Nous utilisons d'abord une propriété de

l'image des morphismes de Cassels-Schaefer énoncée et démontrée au cours de la section 3.3.1. Nous déduisons ensuite de réductions modulo certains éléments premiers de $k[x]$ des conditions de nature arithmétique sur η, ω et ρ sous lesquelles la jacobienne de la courbe hyperelliptique $\mathcal{C}$ d'équation affine

$$\mathcal{C} : z^2 + (y^2+1)(y^2+C(x^2))(y^4+(1+C(x^2))y^2+B(x^2)) = 0$$

est de $\mathbb{R}(x)$-rang de Mordell-Weil nul (voir le théorème 4.6.1). Nous ne donnons pas ces conditions ici. Nous énonçons cependant deux conséquences du théorème 4.6.1.

Théorème 8 *Soient $\eta, \omega, \rho \in \mathbb{R}$ trois nombres réels algébriquement indépendants sur $\mathbb{Q}$. Nous posons :*

$$b_1 = \frac{\rho^2-\eta^2}{\omega^2-\eta^2} + \frac{\eta^2-\omega^2}{4}.$$

Soient $B(x) := (x+b_1)^2 - \eta^2$ et $C(x) := 2(x+b_1) + \omega^2 - \eta^2 - 1$. Nous supposons que $|\omega| > 1 + |\eta|$, $\omega^2 - \eta^2 > 2|\omega|$, et $b_1 > 1 + \frac{\omega^2-\eta^2}{2}$.

Alors le polynôme

$$P(x,y) := \left(y^2+1\right)\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right)$$

est positif ou nul sur $\mathbb{R}^2$, mais n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$.

Théorème 9 *Soient $\eta := 23$, $\omega := 34$ et $\rho := 547$. Nous posons :*

$$b_1 = \tfrac{\rho^2-\eta^2}{\omega^2-\eta^2} + \tfrac{\eta^2-\omega^2}{4} = \tfrac{14063}{44},$$

$$B(x) := (x+b_1)^2 - \eta^2 = x^2 + \tfrac{14063}{22}x + \tfrac{196743825}{1936} \text{ et}$$

$$C(x) := 2(x+b_1) + \omega^2 - \eta^2 - 1 = 2x + \tfrac{27835}{22}.$$

Alors le polynôme

$$P(x,y) := \left(y^2+1\right)\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right) \in \mathbb{Q}(x,y)$$

est positif ou nul sur $\mathbb{R}^2$, mais n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$.

Chapitre 1

Outils généraux.

1.1 Conventions et notations

Nous rappelons tout d'abord quelques définitions concernant les courbes hyperelliptiques.

Définition 1.1.1 *Une courbe hyperelliptique sur un corps k est une courbe $\mathcal{C}$ définie sur k munie d'un morphisme défini sur k, de degré 2 de $\mathcal{C}$ vers $\mathbb{P}^1_k$. Nous disons aussi que $\mathcal{C}$ est une k-courbe hyperelliptique.*

Remarque :
La définition classique impose aux courbes hyperelliptiques d'être de genre supérieur ou égal à 2. La définition proposée est une version élargie : nous utilisons un même formalisme pour étudier les courbes elliptiques et les courbes hyperelliptiques au sens classique (i.e. de genre supérieur ou égal à 2).

Notations 1.1.2 Si $\mathcal{C}$ est une courbe définie sur un corps k, nous notons $k(\mathcal{C})$ le corps de fonctions de $\mathcal{C}$.

Définition 1.1.3 *Soit $\mathcal{C}$ une courbe hyperelliptique sur un corps k et $\varphi : \mathcal{C} \longrightarrow \mathbb{P}^1_k$ le morphisme de degré 2 associé.*

Il existe alors une involution $i : \mathcal{C} \longrightarrow \mathcal{C}$ définie sur k et appelée involution hyperelliptique telle que $\varphi = \varphi \circ i$. L'involution induite par i sur le corps de fonction $k(\mathcal{C})$ de $\mathcal{C}$ est appelée involution hyperelliptique de $k(\mathcal{C})$.

Les points de $\mathcal{C}$ fixés par i sont les points de ramification du morphisme φ.

Remarque :
Si $\mathcal{C}$ est une courbe hyperelliptique sur un corps de caractéristique différente de 2, les points de ramification de $\mathcal{C}$ sont les points de Weierstrass de $\mathcal{C}$.

Proposition 1.1.4 *Toute courbe hyperelliptique sur un corps k de caractéristique différente de 2 admet un modèle affine lisse donné par une équation de la forme*

$$y^2 = f(x)$$

avec f un polynôme à coefficients dans k. L'involution hyperelliptique de $k(\mathcal{C})$ est alors $i : \begin{array}{ccc} k(\mathcal{C}) & \longrightarrow & k(\mathcal{C}) \\ A(x,y) & \longmapsto & A(x,-y) \end{array}$.

Si g désigne le genre de $\mathcal{C}$, alors le degré de f est $2g+1$ ou $2g+2$.

Remarque :

Toutes les courbes hyperelliptiques sont désormais supposées lisses (sauf indication contraire). Lorsque nous parlons de la courbe hyperelliptique d'équation affine $y^2 = f(x)$ (avec $f(x) \in \mathbb{R}[x]$), nous parlons du modèle projectif lisse de la courbe affine plane d'équation $y^2 = f(x)$.

Afin de fixer le vocabulaire, nous précisons également ce que nous entendons par une place d'un corps de fonction :

Définition 1.1.5 *Une place $\mathcal{P}$ d'un corps de fonctions F/k est l'idéal maximal d'un anneau de valuation quelconque $\mathcal{O}_\mathcal{P}$ de F/k.*

Nous notons $F_\mathcal{P} := \mathcal{O}_\mathcal{P}/\mathcal{P}$ le corps résiduel en la place $\mathcal{P}$. L'entier $\deg(\mathcal{P}) := [F_\mathcal{P} : k]$ est appelé degré de $\mathcal{P}$. La classe d'un élément $f \in \mathcal{O}_\mathcal{P}$ dans $F_\mathcal{P}$ est notée $f(\mathcal{P})$.

Soit t une uniformisante de $\mathcal{P}$. Nous normalisons la valuation $v_\mathcal{P}$ associée à $\mathcal{P}$ en posant :

* *$v_\mathcal{P}(0) = \infty$ et*
* *$v_\mathcal{P}(z) = n$ si $z = t^n u$ avec $u \in \mathcal{O}_\mathcal{P}^\times$.*

Notations 1.1.6 Dans ce qui suit nous identifions pour toute courbe lisse $\mathcal{C}$ sur un corps k les points fermés de $\mathcal{C}$ aux places de $k(\mathcal{C})$. Ce faisant nous obtenons les notions

* de groupe des diviseurs de $k(\mathcal{C})$ (noté $\mathrm{Div}(k(\mathcal{C}))$,
* de valuation $v_\mathcal{P}(D)$ d'un diviseur D en une place $\mathcal{P}$ de $k(\mathcal{C})$,
* de support $\mathrm{Supp}(D) = \{\mathcal{P} | v_\mathcal{P}(D) \neq 0\}$ d'un diviseur D,
* de degré $\deg(D) = \sum_\mathcal{P} v_\mathcal{P}(D)$ d'un diviseur D (le groupe des diviseurs de degré 0 de $k(\mathcal{C})$ est noté $\mathrm{Div}^0(k(\mathcal{C}))$,
* de diviseur principal $\mathrm{div}(f) = \sum_\mathcal{P} v_\mathcal{P}(f)\mathcal{P}$ associé à un élément de $f \in k(\mathcal{C})^\times$,
* de groupe des classes de diviseurs de $k(\mathcal{C})$ (noté $\mathrm{Pic}(k(\mathcal{C}))$)
* et de groupe des classes de diviseurs de degré 0 de $k(\mathcal{C})$ (noté $\mathrm{Pic}^0(k(\mathcal{C}))$).

Soit $\overline{k}$ une clôture algébrique de k. Si $D = \sum_{i \in I} n_i \mathcal{P}_i \in \mathrm{Div}^0\left(\overline{k}(\mathcal{C})\right)$ est un diviseur et $f \in \overline{k}(\mathcal{C})$ est une fonction telle que $\mathrm{Supp}(D) \cap \mathrm{Supp}(\mathrm{div}(f)) = \emptyset$, nous définissons $f(D) := \prod_{i \in I} f(\mathcal{P}_i)^{n_i} \in \overline{k}$.

Notations 1.1.7 Soit $\mathcal{C}$ une courbe lisse sur un corps k. Nous notons $\mathrm{div} : k(\mathcal{C})^\times \longrightarrow \mathrm{Div}(k(\mathcal{C}))$ le morphisme qui envoie une fonction sur le diviseur principal associé.

Nous notons $\mathrm{cl} : \mathrm{Div}(k(\mathcal{C})) \longrightarrow \mathrm{Pic}(k(\mathcal{C}))$ le morphisme qui envoie un diviseur sur sa classe d'équivalence linéaire.

Notations 1.1.8 Soit A une variété abélienne sur un corps k. Nous notons $A(k)$ le groupe des points k-rationnels de A.

Soit $n \geq 2$ un entier. Nous notons $[n]$ la multiplication par n de A et $A(k)[n]$ l'ensemble des points de n-torsion du groupe $A(k)$.

1.2 Les sommes de carrés et la notion de points antineutres

Cette partie est consacrée à l'exposition des résultats de [HM01].

Notations 1.2.1 *Soit $\Sigma = Gal(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$. Soit $\boxed{2}_{\mathbb{R}(x)}$ le groupe des sommes non nulles de deux carrés dans $\mathbb{R}(x)$ (nous rappelons que toute fraction positive $F \in \mathbb{R}(x)$ positive ou nulle sur $\mathbb{R}$ est une somme de deux carrés dans $\mathbb{R}(x)$).*

Soient $\mathcal{D}$ une courbe définie sur $\mathbb{R}(x)$, projective, lisse géométriquement intègre, de genre impair, $\mathcal{D}' := \mathcal{D} \times_{Spec(\mathbb{R}(x))} Spec(\mathbb{C}(x))$ sa complexifiée et $p : \mathcal{D}' \longrightarrow \mathcal{D}$ la projection. La courbe $\mathcal{D}'$ est munie d'une action du groupe Σ qui induit une action de Σ sur le groupe de Picard $Pic(\mathbb{C}(x)(\mathcal{D}'))$ de $\mathbb{C}(x)(\mathcal{D}')$.

A la projection p est associé un morphisme p^* de $Pic(\mathbb{R}(x)(\mathcal{D}))$ dans $Pic(\mathbb{C}(x)(\mathcal{D}'))$ dont l'image est contenue dans le sous-groupe $Pic(\mathbb{C}(x)(\mathcal{D}'))^\Sigma$ des élément Σ-invariants de $Pic(\mathbb{C}(x)(\mathcal{D}'))$.

Lemme 1.2.2 *Nous conservons les notations 1.2.1. Nous disposons de la suite exacte :*

$$0 \longrightarrow Pic(\mathbb{R}(x)(\mathcal{D})) \xrightarrow{p^*} Pic(\mathbb{C}(x)(\mathcal{D}'))^\Sigma \xrightarrow{\delta} H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^\times / \mathbb{C}(x)^\times) \longrightarrow 0.$$

Démonstration.

Le noyau de $\mathrm{div} : \mathbb{C}(x)(\mathcal{D}')^\times \longrightarrow \mathrm{Div}(\mathbb{C}(x)(\mathcal{D}'))$ étant $\mathbb{C}(x)^\times$, nous disposons d'une suite exacte courte de Σ-modules :

$$0 \longrightarrow \mathbb{C}(x)(\mathcal{D}')^\times / \mathbb{C}(x)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}(\mathbb{C}(x)(\mathcal{D}')) \xrightarrow{\mathrm{cl}} \mathrm{Pic}(\mathbb{C}(x)(\mathcal{D}')) \longrightarrow 0.$$

Cette suite exacte courte induit une suite exacte longue en cohomologie galoisienne dont nous notons $\delta : \mathrm{Pic}(\mathbb{C}(x)(\mathcal{D}'))^{\Sigma} \longrightarrow H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times})$ le morphisme de cobord,

$$0 \longrightarrow (\mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times})^{\Sigma} \xrightarrow{div} \mathrm{Div}(\mathbb{R}(x)(\mathcal{D})) \xrightarrow{p^*} \mathrm{Pic}(\mathbb{C}(x)(\mathcal{D}'))^{\Sigma}$$
$$\xrightarrow{\delta} H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times}) \longrightarrow H^1(\Sigma, \mathrm{Div}(\mathbb{C}(x)(\mathcal{D}'))). \tag{1.1}$$

Comme $H^1(\Sigma, \mathbb{C}(x)^{\times})$ est nul, la suite exacte courte de Σ-modules :

$$0 \longrightarrow \mathbb{C}(x)^{\times} \longrightarrow \mathbb{C}(x)(\mathcal{D}')^{\times} \longrightarrow \mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times} \longrightarrow 0$$

induit une suite exacte longue en cohomologie galoisienne

$$0 \longrightarrow \mathbb{R}(x)^{\times} \longrightarrow \mathbb{R}(x)(\mathcal{D})^{\times} \longrightarrow (\mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times})^{\Sigma} \longrightarrow 0$$

Ainsi $(\mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times})^{\Sigma}$ est isomorphe à $\mathbb{R}(x)(\mathcal{D})^{\times}/\mathbb{R}(x)^{\times}$.

Soit A un diviseur de $\mathbb{C}(x)(\mathcal{D}')$. Le diviseur A peut s'écrire $A = A^+ - A^-$ avec A^+ et A^- des diviseurs effectifs à supports disjoints. Nous supposons que $\sigma^*(A) = -A$, c'est-à-dire que $\sigma^*(A^+) - \sigma^*(A^-) = A^- - A^+$. Cette dernière égalité se réécrit $A^+ + \sigma^*(A^+) = A^- + \sigma^*(A^-)$. Or les diviseurs A^+, $\sigma^*(A^+)$, A^- et $\sigma^*(A^-)$ sont effectifs et les supports des diviseurs A^+ et A^- sont disjoints, donc $\sigma^*(A^+) = A^-$ et $\sigma^*(A^-) = A^+$. Cela signifie que $A = A^+ - \sigma^*(A^+)$ est dans $Im(1-\sigma)$. Ainsi, le groupe

$$H^1(\Sigma, \mathrm{Div}(\mathbb{C}(x)(\mathcal{D}'))) = \mathrm{Ker}(1+\sigma)/\mathrm{Im}(1-\sigma)$$

est trivial.

Nous rappelons que $\mathrm{Pic}(\mathbb{R}(x)(\mathcal{D}))$ est le quotient de $\mathrm{Div}(\mathbb{R}(x)(\mathcal{D}))$ par $\mathbb{R}(x)(\mathcal{D})^{\times}/\mathbb{R}(x)^{\times}$. Ainsi, en utilisant la propriété universelle du quotient pour le morphisme $p^* : \mathrm{Div}(\mathbb{R}(x)(\mathcal{D})) \longrightarrow \mathrm{Pic}(\mathbb{C}(x)(\mathcal{D}'))^{\Sigma}$, la suite exacte 1.1 devient :

$$0 \longrightarrow \mathrm{Pic}(\mathbb{R}(x)(\mathcal{D})) \xrightarrow{p^*} \mathrm{Pic}(\mathbb{C}(x)(\mathcal{D}'))^{\Sigma} \xrightarrow{\delta} H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times}) \longrightarrow 0. \quad \square .$$

Remarque :

Nous prenons $cl(A) \in \mathrm{Pic}(\mathbb{C}(x)(\mathcal{D}'))^{\Sigma}$ la classe d'un diviseur A. Par Σ-invariance de $cl(A)$, le diviseur $A - \sigma^* A$ est principal et correspond donc au diviseur d'une fonction $f \in \mathbb{C}(x)(\mathcal{D}')^{\times}$. Le diviseur de $\mathbb{R}(x)(\mathcal{D})$ associé à la fonction $f\sigma(f)$ est 0, donc $f\sigma(f) \in \mathbb{R}(x)^{\times}$. Avec ces notations, $\delta(cl(A))$ est la classe de f dans $H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times}) = \mathrm{Ker}(1+\sigma)/\mathrm{Im}(1-\sigma)$.

Notations 1.2.3 *L'application* $1 + \sigma : \mathbb{C}(x)(\mathcal{D}') \longrightarrow \mathbb{R}(x)(\mathcal{D})$ *induit un monomorphisme de groupe* $\eta : H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times}) \longrightarrow \mathbb{R}(x)^{\times}/\boxed{2}_{\mathbb{R}(x)}$ *: si* f *est un représentant d'un élément de* $\in H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times})$*, alors* $\eta(f)$ *est la classe de* $f\sigma(f)$*. Nous posons* $\varpi := \eta \circ \delta$*.*

Lemme 1.2.4 *Soit k un corps de caractéristique différente de 2. Nous supposons que -1 n'est pas une somme de deux carrés dans k. Soit $f \in k$ un élément de k dont l'opposé $-f$ n'est pas un carré dans k. Nous avons alors équivalence entre :*

1. *f est une somme de trois carrés dans k ;*
2. *-1 est une somme de deux carrés dans le corps $k(\sqrt{-f})$.*

De plus, si quatre éléments a_1, a_2, b_1 et b_2 de k vérifient l'égalité $-1 = (a_1 + b_1\sqrt{-f})^2 + (a_2 + b_2\sqrt{-f})^2$, alors

$$f = \left(\frac{b_1}{b_1^2 + b_2^2}\right)^2 + \left(\frac{b_2}{b_1^2 + b_2^2}\right)^2 + \left(\frac{b_1a_2 - b_2a_1}{b_1^2 + b_2^2}\right)^2.$$

Démonstration.

Le cas où f est un carré dans k étant direct, nous supposons que f n'est pas un carré dans k.

Si f est une somme de trois carrés dans k : nous écrivons $f = P_1^2 + P_2^2 + P_3^2$ avec $P_i \in k$. Comme f n'est pas un carré dans k, l'élément $P_2^2 + P_3^2 = f - P_1^2$ est non nul. Nous pouvons donc écrire dans $k(\sqrt{-f})$ l'égalité $-1 = \frac{P_1^2 + \sqrt{-f}^2}{P_2^2 + P_3^2}$. Puisque le quotient de deux sommes de deux carrés est une somme de deux carrés, nous venons d'écrire -1 comme somme de deux carrés dans $k(\sqrt{-f})$.

Si -1 est une somme de deux carrés dans le corps $k(\sqrt{-f})$: nous pouvons écrire $-1 = (a_1 + b_1\sqrt{-f})^2 + (a_2 + b_2\sqrt{-f})^2$ avec a_i, $b_i \in k$. En développant cette égalité, nous obtenons $f(b_1^2 + b_2^2) = 1 + a_1^2 + a_2^2 + 2\sqrt{-f}(b_1a_1 + b_2a_2)$. Puisque $\sqrt{-f}$ n'est pas un élément de k et que la caractéristique de k est différente de 2, cette égalité n'est possible que si $(b_1a_1 + b_2a_2) = 0$; nous avons alors $f(b_1^2 + b_2^2) = 1 + a_1^2 + a_2^2$, c'est-à-dire $f(b_1^2 + b_2^2)^2 = b_1^2 + b_2^2 + (a_1^2 + a_2^2)(b_1^2 + b_2^2)$. Comme $(b_1a_1 + b_2a_2) = 0$, nous savons que $(a_1^2+a_2^2)(b_1^2+b_2^2) = (b_1a_1+b_2a_2)^2+(b_1a_2-b_2a_1)^2 = (b_1a_2-b_2a_1)^2$. Ainsi $f = \left(\frac{b_1}{b_1^2+b_2^2}\right)^2 + \left(\frac{b_2}{b_1^2+b_2^2}\right)^2 + \left(\frac{b_1a_2-b_2a_1}{b_1^2+b_2^2}\right)^2$ est une somme de 3 carrés. □

Définition 1.2.5 *Un élément f d'un anneau A est dit totalement positif si $\varphi(f) > 0$ pour tout morphisme $\varphi : A \longrightarrow K$ où K est un corps réel clos. S'il n'y a pas de tel morphisme, tout élément est totalement positif.*

Proposition 1.2.6 *Soit $P(Y) \in \mathbb{R}(x)[Y]$ totalement positif, unitaire, non constant, sans facteur carré. Soit $\mathcal{D}$ un modèle projectif lisse de la $\mathbb{R}(x)$-courbe plane $\mathcal{C}$ dont une équation affine est $z^2 + P(y) = 0$. Nous avons une équivalence entre :*

1. *$P(Y)$ est une somme de trois carrés dans $\mathbb{R}(x)(Y)$*

2. l'image de ϖ contient -1.

Démonstration.

Dans la démonstration, nous utilisons les objets décrits dans le lemme 1.2.2 et les notations 1.2.3. Par définition de $H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^\times/\mathbb{C}(x)^\times)$, l'image $\mathrm{Im}(\varpi) = \eta(H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^\times/\mathbb{C}(x)^\times))$ contient -1 si et seulement si il existe une fonction $f \in \mathbb{C}(x)(\mathcal{D}')^\times$ telle que $f\sigma(f) = -1$. Toute fonction $f \in \mathbb{C}(x)(\mathcal{D}')^\times$ s'écrit $f = f_1(y)\sqrt{-1} + f_0(y)$ avec $f_i(y) \in \mathbb{R}(x)(\mathcal{D})$. Ainsi l'image $\mathrm{Im}(\eta \circ \delta)$ contient -1 si et seulement si il existe deux fonctions f_1, $f_2 \in \mathbb{R}(x)(\mathcal{D})$ telles que $-1 = (f_1(y)\sqrt{-1} + f_2(y))(-f_1(y)\sqrt{-1} + f_2(y)) = f_1^2 + f_2^2$. Pour finir la démonstration de la proposition 1.2.6, il suffit de faire appel au lemme 1.2.4. □

Lemme 1.2.7 *Soit $P(Y) \in \mathbb{R}(x)[Y]$ totalement positif, unitaire, non constant, sans facteur carré de degré pair. Soit $\mathcal{D}$ un modèle projectif lisse de la $\mathbb{R}(x)$-courbe plane $\mathcal{C}$ dont une équation affine est $z^2 + P(y) = 0$ et $\mathcal{D}'$ sa complexifiée. Nous notons g le genre de $\mathcal{D}$. Soit $A \in Div(\mathbb{C}(x)(\mathcal{D}'))$ un diviseur dont la classe d'équivalence linéaire $cl(A) \in Pic(\mathbb{C}(x)(\mathcal{D}'))$ appartient à $\varpi^{-1}(-1)$ dans $Pic(\mathbb{C}(x)(\mathcal{D}'))^\Sigma$. Alors le degré de A a même parité que $g - 1$.*

Démonstration.

Voir [HM01] lemme 6.4 page 671. □

Proposition 1.2.8 *Soit $P(Y) \in \mathbb{R}(x)[Y]$ totalement positif, unitaire, non constant, sans facteur carré de degré pair. Soit $\mathcal{D}$ un modèle projectif lisse de la $\mathbb{R}(x)$-courbe plane $\mathcal{C}$ dont une équation affine est $z^2 + P(y) = 0$ et $\mathcal{D}'$ sa complexifiée. Nous notons g le genre de $\mathcal{D}$. Nous supposons g impair. Nous notons ϖ^0 la restriction de ϖ à $Pic^0(\mathbb{C}(x)(\mathcal{D}'))^\Sigma$. Alors $P(Y)$ est une somme de trois carrés dans $\mathbb{R}(x)(Y)$ si et seulement si l'image de ϖ^0 contient -1.*

Démonstration.

Voir [HM01] théorème 6.5 page 671. □

Définition 1.2.9 *Nous conservons les notations 1.2.3. Soit $P \in Pic^0(\mathbb{C}(x)(\mathcal{D}'))^\Sigma = Jac(\mathcal{D})(\mathbb{R}(x))$. L'élément P est dit antineutre si $\varpi(P) = -1$.*

Soit $A \in Div(\mathbb{C}(x)(\mathcal{D}'))$ un représentant de la classe d'équivalence linéaire P. Le diviseur A est dit antineutre si $\varpi(P) = -1$.

1.3 Le principe général de l'étude

Soit $P(x, y) \in \mathbb{R}(x)[y]$ un polynôme totalement positif, unitaire, non constant, sans facteur carré de degré divisible par 4. D'après la proposition 1.2.8, le polynôme $P(x, y)$ est une somme de trois carrés dans le corps

$\mathbb{R}(x,y)$ si et seulement si la jacobienne J de la $\mathbb{R}(x)$-courbe hyperelliptique $\mathcal{C}$ d'équation affine $z^2 + P(x,y) = 0$ possède un point $\mathbb{R}(x)$-rationnel antineutre.

La stratégie que nous allons adopter peut se décomposer en deux étapes :

1. montrer que $J(\mathbb{R}(x))$ ne possède aucun élément de torsion antineutre,
2. montrer que le $\mathbb{R}(x)$-rang de Mordell-Weil de la jacobienne J est nul.

Notre attention se porte d'abord sur l'antineutralité des $\mathbb{R}(x)$-points de torsions. Cette étude de l'antineutralité de la torsion $\mathbb{R}(x)$-rationnelle peut être simplifiée :

Proposition 1.3.1 *Soit $P(x,y) \in \mathbb{R}(x)[y]$ totalement positif, unitaire, non constant, sans facteur carré de degré divisible par 4. Soit $\mathcal{C}$ la $\mathbb{R}(x)$-courbe hyperelliptique d'équation affine $z^2 + P(x,y) = 0$. Soit J la jacobienne de la courbe $\mathcal{C}$. Soit D un point $\mathbb{R}(x)$-rationnel de la jacobienne J. Soit $m \in \mathbb{N}$ un entier impair.*

Alors D est antineutre si et seulement si mD est antineutre.

Démonstration.

Nous reprenons les notations 1.2.3. Le morphisme $\eta \circ \delta$ défini est à valeurs dans $\mathbb{R}(x)^\times/\mathbb{R}(x)[2]$ qui est un groupe d'exposant 2. L'image d'un double par $\eta \circ \delta$ est donc toujours triviale. □

D'après cette proposition, l'existence d'un point de torsion de $J(\mathbb{R}(x))$ antineutre est équivalente à l'existence d'un $\mathbb{R}(x)$-point de torsion 2-primaire antineutre. Nous cherchons donc à montrer que :

1. $J(\mathbb{R}(x))$ ne contient aucun élément de torsion 2-primaire antineutre,
2. le $\mathbb{R}(x)$-rang de Mordell-Weil de la jacobienne J est nul.

Au cours du chapitre 2, nous utilisons la notion de représentation de Mumford (exposée dans la section 1.4) pour calculer la torsion 2-primaire de $J(\mathbb{R}(x))$ et nous en déduisons l'existence ou la non existence d'éléments de torsion de $J(\mathbb{R}(x))$ antineutres.

Lors du chapitre 3, nous expliquons comment un choix judicieux des coefficients du polynôme $P(x,y)$ permet de scinder le calcul du $\mathbb{R}(x)$-rang de J en huit études plus simples. En particulier, nous sommes amenés à effectuer une 2-descente en utilisant un lemme de Christie.

La vérification des hypothèses de ce lemme de Christie nécessite de comprendre le quotient $J(\mathbb{R}(x))/2J(\mathbb{R}(x))$. Cela motive l'introduction (au cours de la section 1.5) d'un morphisme de groupes $\pi_{\mathcal{C}}$ de noyau $2J(\mathbb{R}(x))$.

Le chapitre 4 est consacré à la détermination de conditions de nature arithmétique sous-lesquelles le $\mathbb{R}(x)$-rang de Mordell-Weil de J est nul.

1.4 La représentation de Mumford

Le lecteur désirant plus de détails sur la notion de représentation de Mumford pourra consulter [Mum84] ou [Gau00].

Théorème 1.4.1 *Soit $\mathcal{C}$ une courbe sur k projective, lisse, géométriquement intègre, de genre g, avec un point k-rationnel fixé P_0. Soit $D \in Div^0(k(\mathcal{C}))$ un diviseur de degré 0.*

Il existe alors un unique diviseur effectif $E \in Div(k(\mathcal{C}))$ de degré minimal $m \leq g$ tel que D soit équivalent à $E - mP_0$ et $P_0 \notin Supp(E)$.

Démonstration.

Soit $k(\mathcal{C})$ le corps de fonction de la courbe $\mathcal{C}$. Pour tout diviseur D' sur $\mathcal{C}$, nous notons $\mathcal{L}(D') := \{0\} \cup \{h \in k(\mathcal{C}) \mid div(h) \geq -D'\}$ et $l(D') := dim_k(L(D'))$.

Si D est principal, nous prenons $E := 0$ et $m := 0$. Nous supposons maintenant D non principal. Si $l(D) \geq 1$, il existe $h \in k(\mathcal{C})$ tel que $\mathrm{div}(h)+D$ soit effectif. Le diviseur $\mathrm{div}(h)+D$ étant de degré 0, il doit être nul. Ce n'est pas possible car D a été supposé non principal. Par suite $l(D) = 0$.

Soit κ le diviseur canonique de $k(\mathcal{C})$. Par Riemann-Roch, nous avons pour tout m :

$$\begin{aligned} 0 &\leq l(D + (m+1)P_0) - l(D + mP_0) \\ &= l(\kappa - D - (m+1)P_0) + \deg(D + (m+1)P_0) + 1 - g \\ &\quad - (l(\kappa - D - mP_0) + \deg(D + mP_0) + 1 - g) \\ &= l(\kappa - D - (m+1)P_0) - l(\kappa - D - mP_0) + 1. \end{aligned}$$

Or $l(\kappa - D - (m+1)P_0) \leq l(\kappa - D - mP_0)$, donc $l(D + mP_0)$ n'augmente que de 0 ou 1 quand m augmente de 1. Soit $m > 0$ le plus petit entier tel que $l(D + mP_0) > 0$. Nous avons $l(D + mP_0) = 1$ et, si nous notons h l'unique fonction non nulle de $\mathcal{L}(D + mP_0)$ (à multiplication par un scalaire près), $E := div(h) + D + mP_0$ convient. L'unicité de m vient de sa minimalité. □

Proposition 1.4.2 *Soit $\mathcal{C}$ une courbe hyperelliptique sur un corps k de caractéristique différente de 2. Soit g le genre de la courbe $\mathcal{C}$. Nous supposons que $\mathcal{C}$ a un unique point au dessus du point à l'infini de $\mathbb{P}^1$ (qui est k-rationnel), c'est-à-dire qu'une équation affine de $\mathcal{C}$ est de la forme*

$$\mathcal{C} : y^2 = f(x)$$

avec f sans facteur carré et de degré $2g+1$ (que l'on peut choisir unitaire).

Soient $k[\mathcal{C}] := k[x,y]/(y^2 - f(x))$ l'anneau de coordonnées de la partie affine de la k-courbe $\mathcal{C}$ et $I(k[\mathcal{C}])$ le groupe des idéaux fractionnaires de $k[\mathcal{C}]$. Nous notons ∞ l'unique place de $k(\mathcal{C})$ au dessus de la place à l'infini de $k(x)$.

Alors l'application Υ :
$$\begin{array}{ccc} Div^0(k(\mathcal{C})) & \longrightarrow & I(k[\mathcal{C}]) \\ \sum_{i\in J} n_i(\mathcal{P}_i - \deg(\mathcal{P}_i)\infty) & \longmapsto & \prod_{i\in J}(\mathcal{P}_i \cap k[\mathcal{C}])^{n_i} \end{array}$$
est un isomorphisme. Il induit un isomorphisme de $Pic^0(k(\mathcal{C}))$ *dans le groupe des classes d'idéaux de* $k[\mathcal{C}]$.

Démonstration.

Soient S l'ensemble des places de $k[\mathcal{C}]$ différentes de ∞ et $P(k[\mathcal{C}])$ l'ensemble des idéaux premiers de $k[\mathcal{C}]$. Nous savons que l'application $\begin{array}{ccc} S & \longrightarrow & P(k[\mathcal{C}]) \\ \mathcal{P} & \longmapsto & \mathcal{P}\cap k[\mathcal{C}] \end{array}$ est bijective (voir par exemple [Sti93] proposition III.2.9, page 70). Il suffit alors de remarquer que $k[\mathcal{C}]$ est un anneau de Dedekind, pour conclure que Υ est un isomorphisme. $\square$

Proposition 1.4.3 *Nous reprenons les conditions et notations de la proposition 1.4.2. Soient* $\mathcal{P}_1, \cdots, \mathcal{P}_r$ *des places de* $k(\mathcal{C})$ *et* $n_1, \cdots, n_r \in \mathbb{N}$.

Alors les idéaux $\prod_{i=1}^{r}\left(\mathcal{P}_i \bigcap k[\mathcal{C}]\right)^{n_i}$ *et* $\bigcap_{i=1}^{r}\left(\mathcal{P}_i^{n_i} \bigcap k[\mathcal{C}]\right)$ *sont égaux.*

Démonstration.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux de $k[\mathcal{C}]$ de décomposition en idéaux premiers respectivement $\mathfrak{a} = \prod_{\mathfrak{p}\text{ premier}} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{a})}$ et $\mathfrak{b} = \prod_{\mathfrak{p}\text{ premier}} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{b})}$, alors la décomposition en idéaux premiers de $\mathfrak{a}\cap\mathfrak{b}$ est $\mathfrak{a}\cap\mathfrak{b} = \prod_{\mathfrak{p}\text{ premier}} \mathfrak{p}^{\max(n_\mathfrak{p}(\mathfrak{a}), n_\mathfrak{p}(\mathfrak{b}))}$ (voir par exemple [ZS58] chapitre V paragraphe 6 théorème 11). En particulier, $\prod_{i=1}^{r}(\mathcal{P}_i\cap k[\mathcal{C}])^{n_i} = \bigcap_{i=1}^{r}(\mathcal{P}_i\cap k[\mathcal{C}])^{n_i}$ et il suffit de montrer que pour toute place $\mathcal{P}$ de $k(\mathcal{C})$ différente de ∞ et tout $n\in\mathbb{N}$, nous avons $\mathcal{P}^n\cap k[\mathcal{C}] = (\mathcal{P}\cap k[\mathcal{C}])^n$.

Soit $\mathcal{P}$ une place de $k(\mathcal{C})$ différente de ∞. Nous montrons par récurrence l'égalité $\mathcal{P}^n\cap k[\mathcal{C}] = (\mathcal{P}\cap k[\mathcal{C}])^n$. Le cas $n=1$ est direct.

Supposons que l'égalité $\mathcal{P}^{n-1}\cap k[\mathcal{C}] = (\mathcal{P}\cap k[\mathcal{C}])^{n-1}$ soit vraie. Nous écrivons $\mathcal{P}^n\cap k[\mathcal{C}] = \prod_{\mathfrak{p}\text{ premier}} \mathfrak{p}^{n_\mathfrak{p}}$ la décomposition en idéaux premiers de l'idéal $\mathcal{P}^n\cap k[\mathcal{C}]$. Puisque

$$(\mathcal{P}\cap k[\mathcal{C}])^n \subset \mathcal{P}^n\cap k[\mathcal{C}] \subset \mathcal{P}^{n-1}\cap k[\mathcal{C}] = (\mathcal{P}\cap k[\mathcal{C}])^{n-1},$$

nous savons que $n \geq n_{\mathcal{P}\cap k[\mathcal{C}]} \geq n-1$ et $n_\mathfrak{p} = 0$ si $\mathfrak{p} \neq \mathcal{P}\cap k[\mathcal{C}]$ (c.f. [ZS58] chapitre V paragraphe 6 théorème 11). Ainsi $\mathcal{P}^n\cap k[\mathcal{C}]$ est égal à $(\mathcal{P}\cap k[\mathcal{C}])^n$ ou $(\mathcal{P}\cap k[\mathcal{C}])^{n-1} = \mathcal{P}^{n-1}\cap k[\mathcal{C}]$. D'après le théorème d'approximation faible, il existe une uniformisante t de $\mathcal{P}$ appartenant à $k[\mathcal{C}]$. Puisque t^{n-1} appartient

à $\mathcal{P}^{n-1} \cap k[\mathcal{C}]$, mais pas à $\mathcal{P}^n \cap k[\mathcal{C}]$, les idéaux $\mathcal{P}^n \cap k[\mathcal{C}]$ et $(\mathcal{P} \cap k[\mathcal{C}])^{n-1}$ sont différents : $\mathcal{P}^n \cap k[\mathcal{C}] = (\mathcal{P} \cap k[\mathcal{C}])^n$. $\square$

Définition 1.4.4 *Soit k un corps et $\bar{k}$ une cloture algébrique de k. Nous conservons les notations et hypothèses de la proposition 1.4.2. Nous notons $i : k(\mathcal{C}) \longrightarrow k(\mathcal{C})$ l'involution hyperelliptique de $\mathcal{C}$. Elle envoie un élément $A(x,y) \in k(\mathcal{C})$ sur $i(A(x,y)) = A(x,-y)$.*

Un diviseur D de degré 0 de $k(\mathcal{C})$ est dit semi-réduit s'il existe un diviseur effectif E de $k(\mathcal{C})$ de degré $m \in \mathbb{N}$ tel que :

1. *$D = E - m\infty$,*
2. *$\infty \notin Supp(E)$,*
3. *pour toute place non ramifiée $\mathcal{P}$ de $k(\mathcal{C})$, nous avons $\mathcal{P} \notin Supp(E)$ ou $i(\mathcal{P}) \notin Supp(E)$,*
4. *pour toute place $\mathcal{P}$ de $k(\mathcal{C})$ en laquelle l'extension $k(\mathcal{C})/k(x)$ se ramifie, $v_{\mathcal{P}}(E) \in \{0,1\}$.*

L'entier m est appelé poids de D.
Un idéal entier I de $k[\mathcal{C}]$ est dit semi-réduit si $\Upsilon^{-1}(I)$ est un diviseur semi-réduit.

Lemme 1.4.5 *Nous reprenons les conditions et notations de la proposition 1.4.2. Soient $u \in k[x]$ et $v \in k[x]$ deux polynômes tels que u divise $v^2 - f$. Nous supposons que la valuation de u en les facteurs premiers de f est 0 ou 1. Soit $I = (u, y - v)$ l'idéal entier de $k[\mathcal{C}]$ engendré par u et $y - v$.*

Alors $N_{k(\mathcal{C})/k(x)}(I)$ est engendré par u.

Démonstration.

Soit $d := \text{pgcd}(u,v)$. L'idéal $N_{k(\mathcal{C})/k(x)}(I)$ est engendré par $\{N_{k(\mathcal{C})/k(x)}(h) | h \in I\}$. Il contient donc $v^2 - f = N_{k(\mathcal{C})/k(x)}(y - v)$, $u^2 = N_{k(\mathcal{C})/k(x)}(u)$ et $2uv = N_{k(\mathcal{C})/k(x)}(-u + y - v) - u^2 - (v^2 - f)$. Par suite, $v^2 - f$ et ud appartiennent à $N_{k(\mathcal{C})/k(x)}(I)$.

Le polynôme u divise $v^2 - f$. Nous notons μ le polynôme défini par $u\mu = v^2 - f$. Soit $\delta := pgcd(d, \mu)$. Les polynômes ud et $v^2 - f = u\mu$ appartiennent à $N_{k(\mathcal{C})/k(x)}(I)$, donc $u\delta \in N_{k(\mathcal{C})/k(x)}(I)$.

Comme δ divise v, nous avons $v^2 - f \equiv -f \bmod \delta^2$. Or δ divise u et μ, donc δ^2 divise $u\mu = v^2 - f$, et donc δ^2 divise f. Le polynôme f étant sans facteur carré, $\delta = 1$, et donc $N_{k(\mathcal{C})/k(x)}(I)$ contient u.

Si h est un élément de $I = (u, y - v)$, il s'écrit $h = h_u u + h_v(y - v)$ avec h_u, $h_v \in k[\mathcal{C}]$, et, sous ces notations,

$$\begin{aligned} N_{k(\mathcal{C})/k(x)}(h) &= N_{k(\mathcal{C})/k(x)}(h_u u + h_v(y - v)) \\ &= (h_u u + h_v(y - v))(i(h_u)u + i(h_v)(-y - v)) \\ &= (h_u i(h_u)u - h_u i(h_v)(y + v) + i(h_u)h_v(y - v))\, u \\ &\quad + h_v i(h_v)(v^2 - f). \end{aligned}$$

Le polynôme u divisant $v^2 - f$, les éléments de $N_{k(\mathcal{C})/k(x)}(I)$ sont tous divisibles par u. Ainsi, $N_{k(\mathcal{C})/k(x)}(I)$ est engendré par u. $\square$

Proposition 1.4.6 *Nous reprenons les conditions et notations de la proposition 1.4.2. Soient $D \in Div^0(k(\mathcal{C}))$ un diviseur semi-réduit de poids m. Soit $I := \Upsilon(D)$. L'idéal I est un idéal entier de $k[\mathcal{C}]$ et il existe un unique couple $(u, v) \in k[x] \times k[x]$ tel que :*

* *$I = (u, y - v)$,*
* *la valuation de u en les facteurs premiers de f est 0 ou 1,*
* *u est unitaire,*
* *$\deg_x(v) < \deg_x(u)$ et*
* *u divise $v(x)^2 - f(x)$.*

Le couple (u, v) est appelé représentation de Mumford de D. Nous notons $D := div(u, v)$.

Démonstration.

Puisque D est semi-réduit de poids m, le diviseur $D + m\infty$ est effectif. L'idéal I est donc un idéal entier de $k[\mathcal{C}]$. L'ensemble $I \cap k[x]$ est un idéal de $k[x]$. Il est donc principal. Soit u unitaire tel que $I \cap k[x]$ soit l'idéal engendré par u. L'idéal $I/(u)$ est monogène (voir [ZS58] chapitre V paragraphe 1 corollaire 1). Soient $a \in k[x]$ et $b \in k[x]$ deux polynômes tels que la classe dans $k[\mathcal{C}]/(u)$ de l'élément $ay+b \in k[\mathcal{C}]$ engendre l'idéal $I/(u)$. Quitte à multiplier $ay + b$ par un élément inversible de $k[x]/(u)$, nous pouvons supposer que les facteurs premiers de a sont des facteurs premiers de u. Nous pouvons aussi choisir a unitaire.

Soit p un facteur premier commun à a et u. Le polynôme $b^2 - a^2 f = (-ay + b)(ay + b)$ étant un élément de $I \cap k[x]$, il est divisible par u. Le polynôme irréductible p est donc un facteur commun à a et $b^2 - a^2 f$. Par suite, p divise b^2 et donc b. Ainsi, l'idéal $\widetilde{I} := (p)^{-1} I$ est entier (engendré par $\frac{u}{p}$ et $\frac{a}{p}y + \frac{b}{p}$). Soit $\mathcal{P}$ une place de $k(\mathcal{C})$ au dessus de p. Comme $\mathrm{div}(p) = \mathcal{P} + i(\mathcal{P}) - 2\infty$, les valuations de $D = \Upsilon^{-1}(I) = \mathrm{div}(p) + \Upsilon^{-1}(\widetilde{I})$ en $\mathcal{P}$ et $i(\mathcal{P})$ sont strictement positives. Ce n'est pas possible : D est semi-réduit. Par conséquent a et u sont premiers entre eux. Cela signifie que $a = 1$. Soit v le reste de la division euclidienne de $-b$ par u. Nous avons alors $\deg_x(v) < \deg_x(u)$. De plus, l'idéal I est engendré par u et $y - v$.

Le polynôme u divise $b^2 - f$ donc $v^2 - f$. Soit p un facteur premier commun à u et f. Alors p divise $v^2 = (v^2 - f) + f$ donc v^2. Or f est sans facteur carré donc $v^2 - f = N_{k(\mathcal{C})/k(x)}(y - v)$ est de valuation 1 en p. Le polynôme u étant un diviseur de $v^2 - f$, il est de valuation 1 en p.

Nous montrons maintenant l'unicité du couple (u, v). Celle du polynôme u est une conséquence du lemme 1.4.5. Supposons qu'il existe $\widetilde{v} \in k[x]$ tel que $I = (u, y - \widetilde{v})$ et $\deg_x(\widetilde{v}) < \deg_x(u)$. Alors $\widetilde{v} - v = (y - v) - (y - \widetilde{v}) \in I \cap k[x]$ est de degré strictement inférieur à $\deg_x(u)$. Le polynôme u ne peut donc

diviser $\widetilde{v} - v$. La définition de u impose alors à $\widetilde{v} - v$ d'être nul. $\square$

Remarque :

Nous conservons les notations de la proposition 1.4.6. Nous notons $E = D + m\infty$. Le diviseur E est effectif. Nous l'écrivons $E = \sum_i n_i P_i$ avec $P_i = (x_i, y_i) \in \bar{k} \times \bar{k}$.
Les polynômes u et v sont les uniques polynômes vérifiant

* $u(x) = \prod_i (x - x_i)^{n_i}$,
* pour tout i, $v(x_i) = y_i$,
* $\deg_x(v) < m$ et
* u divise $v(x)^2 - f(x)$.

Ainsi, le polynôme u décrit les abscisses des points de E et le polynôme v interpole leurs ordonnées. La condition $u|(v^2 - f)$ permet de tenir compte des multiplicités n_i dans la définition de v.

Proposition 1.4.7 *Nous reprenons les conditions et notations de la proposition 1.4.2. Soit $div(u, v) \in Div^0(k(\mathcal{C}))$ un diviseur semi-réduit. Alors :*

1. *le diviseur $div(u, v) + div(u, -v)$ est le diviseur principal associé a la fonction $u \in k(\mathcal{C})$;*
2. *si u se factorise sous la forme $u = u_1 u_2$ et si v_i est le reste de la division euclidienne de v par u_i, alors $div(u, v) = div(u_1, v_1) + div(u_2, v_2)$.*
3. *le diviseur $div(u, v)$ est de la forme $\mathcal{P} - \deg(\mathcal{P})\infty$ pour une certaine place $\mathcal{P}$ de $k(\mathcal{C})$ si et seulement si u est irréductible.*

Démonstration.

1. Soit p un élément premier de $k[x]$. Le polynôme f est supposé sans facteur carré. Il n'est donc pas divisible par p^2. Par suite, si p divise v, alors p^2 ne divise pas $f - v^2$. Le polynôme p ne peut donc être un facteur commun à v, u et $\frac{v^2-f}{u}$. Ainsi, les polynômes v, u et $\frac{v^2-f}{u}$ sont premiers entre eux dans leur ensemble, et il existe a, b, $c \in k[x]$ tels que $1 = au + bv + c\frac{v^2-f}{u}$ c'est-à-dire tels que $u = au^2 + buv + c(v^2 - f)$. L'idéal

$$\begin{aligned}(u, y - v)(u, y + v) &= (u^2, u(y - v), u(y + v), v^2 - f) \\ &= (u^2, uy, uv, v^2 - f)\end{aligned}$$

contient donc le polynôme u. L'idéal $(u, y - v)(u, y + v)$ est donc l'idéal principal engendré par u.

2. De même les polynômes u_1, u_2 et v doivent être premier entre eux dans leur ensemble (car $u_1u_2|(v^2-f)$). Par conséquent, l'idéal

$$\begin{aligned}(u_1, y-v)(u_2, y-v) &= (u_1u_2, u_1(y-v), u_2(y-v), (y-v)^2)\\ &= (u_1u_2, u_1(y-v), u_2(y-v), f+v^2-2vy)\\ &= \left(u_1u_2, u_1(y-v), u_2(y-v), \tfrac{f-v^2}{u_1u_2}u_1u_2+2v^2-2vy\right)\\ &= (u_1u_2, u_1(y-v), u_2(y-v), v(y-v))\end{aligned}$$

contient le polynôme $y-v$. Nous en déduisons que

$$(u_1, y-v)(u_2, y-v) = (u, y-v).$$

3. Supposons maintenant que le diviseur $\mathrm{div}(u,v)$ de la forme $\mathcal{P}-\deg(\mathcal{P})\infty$ pour une certaine place $\mathcal{P}$ de $k(\mathcal{C})$ c'est-à-dire que l'idéal $(u, y-v)$ est premier. L'anneau $k[\mathcal{C}]$ étant de Dedekind, l'idéal $(u, y-v)$ est maximal. Soit p est un facteur premier unitaire de u. L'idéal $(u, y-v)$ est contenu dans $(p, y-v)$. Par suite $(p, y-v)$ est égal à $(u, y-v)$ (et dans ce cas, d'après le lemme 1.4.5, les polynômes u et p doivent être égaux) ou $(p, y-v)$ est égal à $k[\mathcal{C}]$. Dans ce cas, d'après le lemme 1.4.5, nous avons $p=1$, ce qui contredit l'irréductible de p. Les polynômes u et p sont donc égaux.

Inversement, si u est irréductible alors $N_{k[\mathcal{C}]/k[x]}((u, y-v))$ est un idéal premier. Dans ce cas, par multiplicativité de $N_{k[\mathcal{C}]/k[x]}$, l'idéal $(u, y-v)$ ne peut être un produit de deux idéaux non triviaux de $k[\mathcal{C}]$. □

La proposition suivante explique comment retrouver le poids d'un diviseur semi-réduit à l'aide de sa représentation de Mumford.

Proposition 1.4.8 *Nous reprenons les conditions et notations de la proposition 1.4.2. Soient $D = div(u,v) \in Div^0(k(\mathcal{C}))$ un diviseur semi-réduit de poids m. Alors* $\deg_x(u)$ *est égal à m.*

Démonstration.

Soit $I := \Upsilon(D)$. Comme u engendre $N_{k(\mathcal{C})/k(x)}(I)$ et $N_{k(\mathcal{C})/k(x)}$ est multiplicative, il suffit de prouver la proposition dans le cas où I est un idéal premier, c'est-à-dire lorsque u est irréductible..

Le morphisme d'anneaux $\begin{array}{ccc} k[\mathcal{C}] & \longrightarrow & k[x]/(u) \\ A(x,y) & \longmapsto & A(x,v(x)) \end{array}$ est surjectif. Il induit donc un isomorphisme $k[\mathcal{C}]/I \longrightarrow k[x]/(u)$. L'extension $k[\mathcal{C}]/I$ du corps k est donc de degré $\deg_x(u)$.

La proposition est alors une conséquence de la remarque suivante : le poids d'un diviseur de la forme $\mathcal{P}-m\infty$ (avec $\mathcal{P}$ une place de $k(\mathcal{C})$) est le degré $\deg(\mathcal{P})$ du corps résiduel $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$ en $\mathcal{P}$ (pensé comme extension du corps k). □

Théorème 1.4.9 *Nous conservons les notations de la proposition 1.4.6. Soit D un diviseur de degré* 0.

Il existe alors un unique diviseur semi-réduit $\widetilde{D}$ de degré inférieur ou égal à g tel que D soit linéairement équivalent à $\widetilde{D}$. Le diviseur $\widetilde{D}$ est dit réduit.

Démonstration.

Le théorème 1.4.1 s'applique et nous donne l'existence et l'unicité d'un diviseur effectif E de degré minimal $m \leq g$ tel que D soit linéairement équivalent à $E - m\infty$ et $\infty \notin \mathrm{Supp}(E)$.

Soit $\mathcal{P}$ une place de $k(\mathcal{C})$ en laquelle l'extension $k(\mathcal{C})/k(x)$ ne se ramifie pas. Le diviseur $\mathcal{P}+i(\mathcal{P})-2\infty$ est principal car associé à la fonction $x-x(\mathcal{P})$. Le diviseur E est donc linéairement équivalent à $E-(\mathcal{P}+i(\mathcal{P}))+2\infty$. Ainsi, si $\mathcal{P}$ et $i(\mathcal{P})$ appartiennent à $\mathrm{Supp}(E)$, le diviseur $E-(\mathcal{P}+i(\mathcal{P}))$ est effectif et son existence contredit la minimalité de m.

Si $\mathcal{P} \neq \infty$ est une place de $k(\mathcal{C})$ en laquelle l'extension $k(\mathcal{C})/k(x)$ se ramifie, alors $\mathrm{div}(x-x(\mathcal{P})) = 2\mathcal{P}-2\infty$ et E est donc linéairement équivalent à $E-2\mathcal{P}+2\infty$. Dans ce cas $v_{\mathcal{P}}(E)$ doit être inférieur ou égal à 1 : sinon le diviseur $E-2\mathcal{P}+2\infty$ est effectif et son existence contredit la minimalité de m.

Nous montrons maintenant que $\widetilde{D} := E - m\infty$ est le seul diviseur semi-réduit de degré inférieur à g linéairement équivalent à D. Supposons qu'il existe un diviseur semi-réduit $\widetilde{D}' = E' - m'\infty$ linéairement équivalent à D avec E' effectif et $m' \leq g$. Il existe $\varphi \in k(\mathcal{C})$ telle que $\widetilde{D}' = \widetilde{D} + \mathrm{div}(\varphi)$. Soit (δ, η) la représentation de Mumford de $\widetilde{D}$. Le diviseur principal associé à δ est $\mathrm{div}(\delta) = E + i(E) - 2m\infty$. Le diviseur associé à $\varphi\delta$ est donc $\mathrm{div}(\varphi\delta) = E' + i(E) - (m+m')\infty$. Par suite, la fonction $\varphi\delta$ n'a de pôle qu'en l'infini : cette fonction est polynomiale et s'écrit $\sigma(x) + y\tau(x)$ avec σ, $\tau \in k[x]$. La valuation de y en ∞ est $2g+1$ (donc impaire) et celle de x est 2. Ainsi, pour des raisons de parité, $v_\infty(\sigma(x))$ et $v_\infty(y\tau(x))$ ne peuvent être égales. Puisque $v_\infty(\varphi\delta)$ est inférieure à $2g$ (car $m \leq g$ et $m' \leq g$), τ doit être nul. Par conséquent $\varphi = \frac{\varphi\delta}{\delta} = \frac{\sigma}{\delta}$ est une fraction rationnelle en x et le passage de $\widetilde{D}$ à $\widetilde{D}'$ ne s'effectue qu'en ajoutant ou retranchant des diviseurs principaux du type $\mathrm{div}(x - x(\mathcal{P})) = \mathcal{P} + i(\mathcal{P}) - 2\infty$ ($\mathcal{P}$ désignant une place de $k(\mathcal{C})$). Les diviseurs $\widetilde{D}$ et $\widetilde{D}'$ étant semi-réduits, nous avons une contradiction si $\widetilde{D} \neq \widetilde{D}'$. $\square$

Définition 1.4.10 *Nous conservons les notations de la proposition 1.4.6. Soit $P \in Pic^0(k(\mathcal{C}))$. D'après le théorème 1.4.9, la classe d'équivalence linéaire P contient un unique diviseur réduit D. Soit (u, v) la représentation de Mumford de D. Le couple (u, v) est appelé représentation de Mumford de P et nous notons $P =< u, v >$.*

Remarque :

La courbe $\mathcal{C}$ possédant un point rationnel, nous pouvons identifier $\mathrm{Jac}(\mathcal{C})(k)$ et $\mathrm{Pic}^0(k(\mathcal{C}))$. Nous obtenons ainsi la notion de représentation de Mumford d'un élément de $\mathrm{Jac}(\mathcal{C})(k)$.

Nous expliquons maintenant comment calculer dans la jacobienne d'une courbe hyperelliptique à l'aide des représentations de Mumford. L'algorithme présenté ci-dessous est dû à Cantor. Il s'inspire de l'algorithme de réduction de Gauss pour les formes quadratiques. Nous y distinguons deux parties : un algorithme d'addition des diviseurs semi-réduits et un algorithme de réduction des diviseurs semi-réduits.

Nous conservons les notations de la proposition 1.4.6. Soient $D_1 = \mathrm{div}(u_1, v_1)$ et $D_2 = \mathrm{div}(u_2, v_2)$ deux diviseurs semi-réduits.

Nous posons $d = \mathrm{pgcd}(u_1, u_2, v_1 + v_2)$. Il existe s_1, s_2, $s_3 \in k[x]$ tels que $d = s_1u_1 + s_2u_2 + s_3(v_1 + v_2)$. Le diviseur $D_1 + D_2$ n'est pas semi-réduit en général. Cependant, le polynôme d a été défini de telle façon que la diviseur $D_3 := D_1 + D_2 - \mathrm{div}(d)$ soit semi-réduit. Sa représentation de Mumford est (u_3, v_3) avec $u_3 = \frac{u_1u_2}{d^2}$ et v_3 obtenu par application du lemme chinois. L'algorithme de Cantor commence ainsi par :

Algorithme 1.4.11.1 Algorithme d'addition de Cantor.

ENTRÉE: Deux diviseurs semi-réduits $D_1 = \mathrm{div}(u_1(x), v_1(x))$ et $D_2 = \mathrm{div}(u_2(x), v_2(x))$.
SORTIE: Un diviseur semi-réduit $D_3 = \mathrm{div}(u_3(x), v_3(x))$ linéairement équivalent à $D_1 + D_2$.

---

1. Par un algorithme d'Euclide étendu, calculer d, s_1, s_2 et s_3 tels que
$d = \mathrm{pgcd}(u_1, u_2, v_1 + v_2) = s_1u_1 + s_2u_2 + s_3(v_1 + v_2)$;
2. $u_3 \longleftarrow \frac{u_1u_2}{d^2}$;
3. $v_3 \longleftarrow (s_1u_1v_2 + s_2u_2v_1 + s_3u_3(v_1v_2 + f))/d \bmod u_3$;
4. Retourner $\mathrm{div}(u_3, v_3)$.

Nous simplifions maintenant la réduction d'un diviseur semi-réduit. Nous considérons un diviseur $D = \mathrm{div}(u, v)$ semi-réduit que nous supposons non réduit. Cantor propose d'effectuer la réduction grâce à l'algorithme suivant :

Algorithme 1.4.11.2 Algorithme de réduction de Cantor.

ENTRÉE: Un diviseur semi-réduit $D = \mathrm{div}(u, v)$.
SORTIE: L'unique diviseur réduit D' linéairement équivalent à D.

---

1. Tant que $\deg_x(u) > g$ **Faire**
$\lambda \longleftarrow$ le coefficient dominant de $f - v^2$;
$u \longleftarrow \frac{f-v^2}{\lambda u}$;
$v \longleftarrow -v \bmod u$;
2. Retourner le diviseur $D' = \mathrm{div}(u, v)$.

Cet algorithme consiste à utiliser l'algorithme d'addition de Cantor pour le diviseur $D = \mathrm{div}(u, v)$ et le diviseur principal $\mathrm{div}(y+v) = \mathrm{div}(f-v^2, -v)$. Comme $\deg_x(u) \geq g+1$, $\deg_x(f) = 2g+1$ et $\deg_x(u) > \deg_x(v)$, le degré de u^2 est strictement supérieur à celui de $f-v^2$ et donc $\deg_x\left(\frac{f-v^2}{u}\right) < \deg_x(u)$. Ainsi, $\mathrm{div}(\frac{f-v^2}{u}, -v \bmod u)$ est de poids strictement inférieur au poids de $D = \mathrm{div}(u, v)$.

Proposition 1.4.12 *Nous conservons les notations de la proposition 1.4.6.*

Les points de 2-torsion de $Jac(\mathcal{C})(k)$ sont les $< u, 0 >$ avec $u \in k[x]$ un diviseur de f de degré inférieur ou égal à g.

Démonstration.

Soit $P =< u, v >$ un élément de 2-torsion de $\mathrm{Jac}(\mathcal{C})(k)$. Il existe $h \in k(\mathcal{C})$ tel que $2\mathrm{div}(u, v) = \mathrm{div}(h)$. Nous écrivons $h = ay + b$, avec a, $b \in k(x)$. D'après le lemme 1.4.5, les polynômes $b^2 - a^2 f = N_{k(\mathcal{C})/k(x)}(h)$ et u^2 sont égaux à multiplication par un élément de $k^\times$ près. Ainsi, le polynôme $b^2 - a^2 f$ est de degré inférieur à $2g$. Or f est de degré $2g+1$, donc $a = 0$. Par suite, $2\mathrm{div}(u, v) = \mathrm{div}(u) = \mathrm{div}(u, v) + i(\mathrm{div}(u, v))$ et donc $\mathrm{div}(u, v)$ est invariant sous i : son support n'est constitué que de places de $k(\mathcal{C})$ en lesquelles l'extension $k(\mathcal{C})/k(x)$ se ramifie. □

1.5 Une caractérisation des doubles dans les jacobiennes de courbes hyperelliptiques

Dans cette section, nous construisons le morphisme de Cassels-Schaefer. Il caractérise les doubles dans les jacobiennes de courbes hyperelliptiques d'équation de la forme $y^2 = f(x)$ avec $f(x)$ un polynôme séparable, unitaire de degré impair. Sa construction est reprise des articles [Sch95] et [Sch98].

Notations 1.5.1 Soient K un corps de caractéristique 0 et $\overline{K}$ une cloture algébrique de K. Nous notons $G := \mathrm{Gal}(\overline{K}/K)$
Nous considérons une courbe hyperelliptique $\mathcal{C}$ sur K donnée par une équation affine de la forme

$$\mathcal{C} : y^2 = f(x) \text{ avec } f(x) \text{ séparable, unitaire de degré impair.}$$

Nous notons $J := \mathrm{Jac}(\mathcal{C})$.

Soit g le genre de la courbe $\mathcal{C}$. Le polynôme $f(x)$ est de degré $2g+1$. Nous notons $(\alpha_i)_{i=1}^{2g+1}$ ses racines dans $\overline{K}$. Soient ∞ l'unique point de $\mathcal{C}$ au dessus du point à l'infini de $\mathbb{P}^1$ et $P_i = (\alpha_i, 0)$ pour $i = 1, \cdots, 2g+1$. Soient $W := \{P_1, \cdots, P_{2g+1}, \infty\}$ l'ensemble des points de ramification de $\mathcal{C}$ et

$$\mathrm{Div}^0_W(K(\mathcal{C})) := \{D \in \mathrm{Div}(K(\mathcal{C})) \mid \deg(D) = 0, \mathrm{Supp}(D) \cap W = \emptyset\}.$$

Notations 1.5.2 Soit $L := K[T]/(f(T))$, $\overline{L} := \overline{K}[T]/(f(T))$, $A := L^\times/L^{\times 2}$ et $\overline{A} := \overline{L}^\times/\overline{L}^{\times 2}$. La classe d'un élément u de $K[T]$ dans A sera notée $[u]$.

Nous définissons un morphisme de groupe

$$\begin{array}{rccc} \phi: & \mathrm{Div}_W^0(K(\mathcal{C})) & \longrightarrow & A \\ & \sum_{i\in I} n_i Q_i & \longmapsto & \left[\prod_{i\in I}(x(Q_i)-T)^{n_i}\right] \end{array}.$$

Lemme 1.5.3 *Soit $\mathcal{P}$ est une place de $K(\mathcal{C})$ de représentation de Mumford (u,v) avec pgcd$(u,f)=1$.*

Alors $\mathcal{P} - \deg(\mathcal{P})\infty$ est équivalent à un élément D de $Div_W^0(K(\mathcal{C}))$ et $\phi(D) = [(-1)^{\deg_x(u)}u(T)]$.

Démonstration.

Soit $\mathcal{Q}_1$ une place de $\overline{K}(\mathcal{C})$ au dessus de $\mathcal{P}$. Nous notons $r := \deg(\mathcal{P})$. Il existe $\sigma_1, \cdots, \sigma_r \in G$ tels que le diviseur $\mathcal{P} - r\infty$ s'écrive $\sum_{i=1}^{r}(\sigma_i(\mathcal{Q}_1) - \infty)$ dans $\mathrm{Div}^0(\overline{K}(\mathcal{C}))$. Nous posons $h := \prod_{i=1}^{r}(y - \sigma_i(y(\mathcal{Q}_1))) \in K(\mathcal{C})$. Le diviseur $\mathrm{div}(h)$ est un diviseur principal de $K(\mathcal{C})$.

Nous notons $\mathcal{Q}_1, \cdots, \mathcal{Q}_{2g+1}$ les places de $\overline{K}(\mathcal{C})$ (avec multiplicités) telles que $\mathrm{div}(y - y(\mathcal{Q}_1)) = \sum_{j=1}^{2g+1} \mathcal{Q}_i$. Nous désignons par inv l'involution hyperelliptique de $\overline{K}(\mathcal{C})$. Nous avons alors :

$$\mathrm{div}(h) = \left(\sum_{i=1}^{r}\sum_{j=1}^{2g+1}\sigma_i(\mathcal{Q}_j)\right) - (2g+1)r\infty \text{ et}$$

$$\mathrm{div}(u) = \left(\sum_{i=1}^{r}\sigma_i(\mathcal{Q}_1)\right) + \left(\sum_{i=1}^{r}\sigma_i(inv(\mathcal{Q}_1))\right) - 2r\infty.$$

Finalement, le diviseur

$$\begin{array}{rcl} D & = & \mathcal{P} - r\infty + \mathrm{div}\left(\frac{u^g}{h}\right) \\ & = & \sum_{i=1}^{r}(g\sigma_i(\mathcal{Q}_1) + g\sigma_i(inv(\mathcal{Q}_1)) - \sigma_i(\mathcal{Q}_2) - \cdots - \sigma_i(\mathcal{Q}_{2g+1})) \end{array}$$

appartient à $\mathrm{Div}_W^0(K(\mathcal{C}))$.

Nous utilisons l'égalité $x(\mathcal{Q}_1) = x(i(\mathcal{Q}_1))$ pour montrer que

$$\begin{aligned}
\phi(D) &= \left[\prod_{i=1}^{r} \frac{(x(\sigma_i(\mathcal{Q}_1)) - T)^{2g+1}}{(x(\sigma_i(\mathcal{Q}_1)) - T)\cdots(x(\sigma_i(\mathcal{Q}_{2g+1})) - T)}\right] \\
&= \left[\prod_{i=1}^{r} \frac{(x(\sigma_i(\mathcal{Q}_1)) - T)^{2g+1}}{y(\sigma_i(\mathcal{Q}_1))^2 - f(T)}\right] \\
&= \left[\prod_{i=1}^{r} \frac{(x(\sigma_i(\mathcal{Q}_1)) - T)^{2g+1}}{y(\sigma_i(\mathcal{Q}_1))^2}\right] \\
&= [\prod_{i=1}^{r}(x(\sigma_i(\mathcal{Q}_1)) - T)] \\
&= [(-1)^{\deg_x(u)}u(T)]. \quad \square
\end{aligned}$$

Proposition 1.5.4 *L'application ϕ définit par passage au quotient un morphisme $\Phi : J(K) \longrightarrow A$.*

Démonstration.

Soient D_1, $D_2 \in \mathrm{Div}^0_W(K(\mathcal{C}))$ deux diviseurs linéairement équivalents. Nous voulons montrer que $\phi(D_1 - D_2) = 1_A$. Soit $h \in K(\mathcal{C})$ tel que $\mathrm{div}(h) = D_1 - D_2$. D'après la loi de réciprocité de Weil (voir [Sil92]), nous avons pour tout $i = 1, \cdots, 2g+1$

$$(x-\alpha_i)(D_1-D_2) = (x-\alpha_i)(\mathrm{div}(h)) = h(\mathrm{div}(x-\alpha_i)) = h(2P_i-2\infty) = h(P_i-\infty)^2.$$

Par le lemme chinois, $\phi(D_1 - D_2)$ est donc l'élément trivial de $\overline{A}$. Ainsi $\phi(D_1 - D_2)$ est l'élément trivial de A.

Par ailleurs, tout diviseur $D \in \mathrm{Div}^0(K(\mathcal{C}))$ est linéairement équivalent à un élément de $\mathrm{Div}^0_W(K(\mathcal{C}))$. L'application ϕ définit donc bien par passage au quotient un morphisme $\Phi : J(K) \longrightarrow A$. $\square$

Notations 1.5.5 Nous rappelons que G désigne le groupe de Galois $Gal(\overline{K}/K)$. Nous disposons d'une suite exacte courte

$$0 \longrightarrow J(\overline{K})[2] \longrightarrow J(\overline{K}) \xrightarrow{[2]} J(\overline{K}) \longrightarrow 0.$$

Cette suite exacte courte induit une suite exacte longue en cohomologie :

$$\begin{aligned}
&0 \longrightarrow J(K)[2] \longrightarrow J(K) \xrightarrow{[2]} J(K) \xrightarrow{\delta} \mathrm{H}^1(G, J(\overline{K})[2]) \\
&\longrightarrow \mathrm{H}^1(G, J(\overline{K})) \xrightarrow{[2]} \mathrm{H}^1(G, J(\overline{K})).
\end{aligned}$$

Nous en déduisons par passage au quotient du morphisme δ une suite exacte

$$0 \longrightarrow J(K)/2J(K) \xrightarrow{\tilde{\delta}} \mathrm{H}^1(G, J(\overline{K})[2]) \longrightarrow \mathrm{H}^1(G, J(\overline{K}))[2] \longrightarrow 0,$$

où $\mathrm{H}^1(G, J(\overline{K}))[2]$ désigne le noyau de l'application

$$[2] : \mathrm{H}^1(G, J(\overline{K})) \longrightarrow \mathrm{H}^1(G, J(\overline{K})).$$

Le morphisme $\tilde{\delta}$ nous permet de caractériser $2J(K)$. Nous allons maintenant le relier au morphisme Φ défini précédemment. Pour cela, nous utilisons l'accouplement de Weil e_2. Nous rappelons la définition de cet accouplement donné dans [Har82] (elle sera utile dans les calculs qui suivent) :

Définition 1.5.6 *Nous conservons les notations 1.5.1 et 1.5.2. Soient $T_1 \in Pic^0(\overline{K}(\mathcal{C}))$ et $T_1 \in Pic^0(\overline{K}(\mathcal{C}))$ deux éléments de 2-torsion de $Pic^0(\overline{K}(\mathcal{C}))$. Soient $D_1 \in Div^0(\overline{K}(\mathcal{C}))$ et $D_2 \in Div^0(\overline{K}(\mathcal{C}))$ des représentants de T_1 et T_2 respectivement tels que $Supp(T_1) \cap Supp(T_2) = \emptyset$. Par définition, il existe deux fonctions h_1, $h_2 \in \overline{K}(\mathcal{C})$ telles que $2D_1 = div(h_1)$ et $2D_2 = div(h_2)$.*

Nous posons alors $e_2(T_1, T_2) := \frac{h_2(D_1)}{h_1(D_2)}$. L'accouplement

$$e_2 : J(\overline{K})[2] \times J(\overline{K})[2] \longrightarrow \mu_2(\overline{K})$$

ainsi défini est appelé accouplement de Weil.

Nous notons également $w : \begin{array}{ccc} J(\overline{K})[2] & \longrightarrow & \prod_{l=1}^{2g+1} \mu_2(\overline{K}) \\ T & \longmapsto & (e_2(T, P_i - P_\infty))_{i=1}^{2g+1} \end{array}$. *En fait, par le lemme chinois, w peut être vu comme une application $w : J(\overline{K})[2] \longrightarrow \mu_2(\overline{L})$ où $\overline{L} := \overline{K}[T]/(f(T))$.*

Remarques :

1. L'accouplement de Weil e_2 est bien à valeurs dans $\mu_2(\overline{K})$ car

$$\begin{array}{rcl} \left(\frac{h_2(T_1)}{h_1(T_2)}\right)^2 & = & \frac{h_2(2T_1)}{h_1(2T_2)} \\ & = & \frac{h_2(\mathrm{div}(h_1))}{h_1(\mathrm{div}(h_2))} \\ & = & 1 \text{ (par application de la loi de réciprocité de Weil).} \end{array}$$

2. Nous obtenons la structure de $\mathrm{Gal}(\overline{K}/K)$-module de $\overline{L}$ en faisant agir $\mathrm{Gal}(\overline{K}/K)$ trivialement sur T.

   Cette structure peut aussi être obtenue en transportant la structure de $\mathrm{Gal}(\overline{K}/K)$-module de $\prod_{l=1}^{2g+1} \mu_2(\overline{K})$ suivante. Soit σ est un élément de $\mathrm{Gal}(\overline{K}/K)$. L'élément σ induit une permutation $\tau \in \mathfrak{S}_{2g+1}$ telle que σ envoie α_i sur $\alpha_{\tau(i)}$. L'action de σ associe à un élément $\beta = (\beta_i)_{i=1}^{2g+1}$ l'élément $\tau(\beta) = \left(\sigma\left(\beta_{\tau^{-1}(i)}\right)\right)_{i=1}^{2g+1}$.

Proposition 1.5.7 *Nous conservons les notations 1.5.1 et 1.5.2. L'accouplement de Weil e_2 est $\mathbb{Z}$-bilinéaire en les deux variables, anti-symétrique (et aussi symétrique), non dégénéré et invariant sous Galois (c'est-à-dire que pour tout $\sigma \in G$, nous avons $\sigma(e_2(T_1, T_2)) = e_2(\sigma(T_1), \sigma(T_2))$).*

En particulier, l'application $w : J(\overline{K})[2] \longrightarrow \mu_2(\overline{L})$ est injective et G-invariante ($\forall \sigma \in G, w \circ \sigma = \sigma \circ w$).

L'application $w : J(\overline{K})[2] \longrightarrow \mu_2(\overline{L})$ définit par fonctorialité une application $w : \mathrm{H}^1(G, J(\overline{K})[2]) \longrightarrow \mathrm{H}^1(G, \mu_2(\overline{L}))$.

Il nous faut encore définir une dernière application : d'après la théorie de Kummer ([Ser68]), nous avons un isomorphisme $k : H^1(G, \mu_2(\overline{L})) \longrightarrow A$. En effet, la suite exacte courte

$$0 \longrightarrow \mu_2(\overline{L}) \longrightarrow \overline{L}^\times \xrightarrow{\times 2} \overline{L}^\times \longrightarrow 0$$

induit une suite exacte longue en cohomologie :

$$0 \longrightarrow \mu_2(L) \longrightarrow L^\times \xrightarrow{\times 2} L^\times \xrightarrow{\Delta} \mathrm{H}^1(G, \mu_2(\overline{L})) \longrightarrow \mathrm{H}^1(G, \overline{L}^\times) \longrightarrow \cdots$$

D'après le théorème d'Hilbert 90, le groupe $\mathrm{H}^1(G, \overline{L}^\times)$ est trivial. Nous en déduisons par passage au quotient du morphisme Δ un isomorphisme k^{-1} : $A \longrightarrow H^1(G, \mu_2(\overline{L}))$. Si $a \in L^\times$ et si $\tilde{a}$ est une racine carrée de a dans $\overline{L}$, alors pour tout $\sigma \in G$, $k^{-1}(a)(\sigma) = \frac{\sigma(\tilde{a})}{\tilde{a}}$.

Lemme 1.5.8 *Les applications Φ et $k \circ w \circ \delta$ sont égales.*

Démonstration.

Soient $P \in J(K) \simeq \mathrm{Pic}^0(K(\mathcal{C}))$ et $Q \in J(\overline{K}) \simeq \mathrm{Pic}^0(\overline{K}(\mathcal{C}))$ tel que $[2]Q = P$. D'après le lemme 1.5.3, il existe deux diviseurs $D_1 \in \mathrm{Div}^0_W(K(\mathcal{C}))$, $D_2 \in \mathrm{Div}^0_W(\overline{K}(\mathcal{C}))$ de classes d'équivalence linéaire respectivement P et Q. Nous pouvons de plus supposer D_1 invariant sous G. Soit $h \in \overline{K}(\mathcal{C})$ avec $\mathrm{div}(h) = 2D_2 - D_1$.

Le morphisme δ est explicitement défini : l'image de D_1 par δ est la classe de cohomologie associée au cocycle $\begin{array}{ccc} G & \longrightarrow & J(\overline{K})[2] \\ \sigma & \longmapsto & \sigma(D_2) - D_2 \end{array}$.

Par conséquent $w \circ \delta(P)$ est la classe de cohomologie associée au cocycle

$$\begin{array}{ccc} G & \longrightarrow & \mu_2(\overline{L})) \simeq \prod_{l=1}^{2g+1} \mu_2(\overline{K}) \\ \sigma & \longmapsto & (e_2(\sigma(D_2) - D_2, P_l - \infty))_{l=1}^{2g+1} \end{array}.$$

Comme D_1 est invariant sous G et $\mathrm{div}(h) = 2D_2 - D_1$, nous avons

$$\begin{aligned} \mathrm{div}\left(\tfrac{\sigma(h)}{h}\right) &= (2\sigma(D_2) - \sigma(D_1)) - (2D_2 - D_1) \\ &= 2\sigma(D_2) - 2D_2. \end{aligned}$$

De plus, $\mathrm{div}(x - \alpha_l) = 2(P_l - \infty)$, donc

$$e_2(\sigma(D_2) - D_2, P_l - \infty) = \frac{(x - \alpha_l)((\sigma(D_2) - D_2)}{(\sigma(h)/h)(P_l - \infty)} \frac{\sigma(\beta)}{\beta} = k^{-1}(\beta^2)$$

où β est l'élément de $H^1(G, \mu_2(\overline{L}))$ associé au $(2g+1)$-uplet $\left(\frac{(x-\alpha_l)(D_2)}{h(P_l-\infty)}\right)_{l=1}^{2g+1}$.

Cela signifie que $k \circ w \circ \delta(P) = \beta^2 = \left(\frac{(x-\alpha_l)(2D_2)}{h(2P_l-2\infty)}\right)_{l=1}^{2g+1}$. Nous déduisons de la loi de réciprocité de Weil que $h(2P_l - 2\infty) = (x - \alpha_l)(2D_2 - D_1)$, et donc que $k \circ w \circ \delta(P) = \left(\frac{(x-\alpha_l)(2D_2)}{(x-\alpha_l)(2D_2-D_1)}\right)_{l=1}^{2g+1} = ((x - \alpha_l)(D_1))_{l=1}^{2g+1}$. $\square$

Proposition 1.5.9 *L'application k∘w est un isomorphisme du groupe* $H^1(G, J(\overline{K}[2]))$ *dans le noyau de la norme* $N_{K/L} : L^\times/L^{\times 2} \longrightarrow K^\times/K^{\times 2}$.

Démonstration.

L'image de $w : J(\overline{K})[2] \longrightarrow \mu_2(\overline{L})$ est contenue dans le noyau de la norme $N_{\overline{K}/\overline{L}} : \mu_2(\overline{L}) \longrightarrow \mu_2(\overline{K})$: si $T \in J(\overline{K})[2]$, alors

$$\begin{aligned} N_{\overline{K}/\overline{L}}(w(T)) &= \prod_{i=1}^{2g+1} e_2(T, P_i - \infty) \\ &= e_2(T, \sum_{i=1}^{2g+1}(P_i - \infty)) \\ &= e_2(T, 0) = 1. \end{aligned}$$

De plus, les $\mathbb{Z}/2\mathbb{Z}$-espaces vectoriels $J(\overline{K})[2]$, $\mu_2(\overline{L})$ et $\mu_2(\overline{K})$ sont dimensions respectives $2g$, $2g+1$ et 1. Nous disposons donc de la suite exacte de G-modules suivante :

$$0 \longrightarrow J(\overline{K})[2] \xrightarrow{w} \mu_2(\overline{L}) \xrightarrow{N_{\overline{L}/\overline{K}}} \mu_2(\overline{K}) \longrightarrow 1 \ .$$

La suite exacte longue en cohomologie induite est

$$\cdots \longrightarrow \mu_2(L) \xrightarrow{N_{K/L}} \mu_2(K) \longrightarrow H^1(G, J(\overline{K})[2]) \xrightarrow{w} H^1(G, \mu_2(\overline{L}))$$

$$\xrightarrow{N_{\overline{K}/\overline{L}}} H^1(G, \mu_2(\overline{K})) \longrightarrow \cdots$$

En particulier, $\mathrm{Im}(w : H^1(G, J(\overline{K})[2]) \longrightarrow H^1(G, \mu_2(\overline{L})))$ est égal à $\mathrm{Ker}(N_{\overline{K}/\overline{L}} : H^1(G, \mu_2(\overline{L})) \longrightarrow H^1(G, \mu_2(\overline{K})))$.

Puisque $N_{K/L}(-1) = (-1)^{2g+1} = -1$, la norme $N_{K/L} : \mu_2(L) \longrightarrow \mu_2(K)$ est surjective. Par conséquent le morphisme $w : H^1(G, J(\overline{K})[2]) \longrightarrow H^1(G, \mu_2(\overline{L}))$ est injectif. Pour conclure il suffit de remarquer que le diagramme suivant est commutatif :

$$\begin{array}{ccccc} 0 & \longrightarrow & H^1(G, \mu_2(\overline{L})) & \xrightarrow{k} & L^\times/L^{\times 2} \longrightarrow 1 \\ & & \Big\downarrow{\scriptstyle N_{\overline{L}/\overline{K}}} & & \Big\downarrow{\scriptstyle N_{L/K}} \\ 0 & \longrightarrow & H^1(G, \mu_2(\overline{K})) & \xrightarrow{k} & L^\times/L^{\times 2} \longrightarrow 1 \end{array} \qquad \square$$

Théorème 1.5.10 *Le noyau de* Φ *est égal à* $2J(K)$.

Démonstration.

D'après la proposition 1.5.9, l'application $k \circ w$ est un isomorphisme. Par ailleurs, l'application $\widetilde{\delta}$ est une injection, donc l'application $k \circ w \circ \widetilde{\delta}$ est injective. Par suite le noyau de $\Phi = k \circ w \circ \delta$ est bien $2J(K)$. $\square$

Chapitre 2

Etude de la torsion 2-primaire de deux familles de courbes

2.1 Un changement de variable permettant de représenter les points de la jacobienne.

Soit k un sous-corps de $\mathbb{R}$. Soit $k' := k(i)$. Nous notons σ la conjugaison complexe sur k et $\Sigma = \mathrm{Gal}(k'/k) = \{1, \sigma\}$.

Soient $Q(T) \in k(x)[T]$ un polynôme unitaire de degré g et $P(T) := (T+1)Q(T)$. Nous supposons $Q(-1)$ non nul et $P(y^2)$ sans facteur carré. Soit $\mathcal{C}$ la $k(x)$-courbe hyperelliptique d'équation affine

$$\mathcal{C} : z^2 + P(y^2) = 0.$$

Nous souhaitons représenter de manière effective les éléments de $\mathrm{Jac}(\mathcal{C})(k(x))$ à l'aide de la représentation de Mumford. Malheureusement, le polynôme P est de degré pair et nous ne pouvons appliquer les résultats de la section 1.4. Cependant la courbe $\mathcal{C}$ est isomorphe sur $k'(x)$ à une courbe $\widetilde{\mathcal{C}}$ donnée par une équation affine de la forme $t^2 = f(s)$ avec $f(s) \in k(x)[s]$ un polynôme de degré impair en s. Cette courbe $\widetilde{\mathcal{C}}$ est obtenue en envoyant à l'infini un point de ramification $k'(x)$-rationnel P_0 de $\mathcal{C}$. Le fait que P_0 soit un point de ramification est crucial : étant donnée son équation, la courbe hyperelliptique $\widetilde{\mathcal{C}}$ doit avoir un unique point au dessus du point à l'infini de $\mathbb{P}^1$.

Nous mettons en évidence un point $k'(x)$-rationnel.

La courbe $\mathcal{C}$ ne possède pas de point de ramification $k(x)$-rationnel en général : ces points ont pour abscisses les racines dans $k(x)$ du polynôme P. Nous devons donc commencer par réaliser un premier changement de variable qui malheureusement ne définit pas un isomorphisme sur $k(x)$ mais seulement sur $k'(x)$.

Soit $\mathcal{D}$ la $k(x)$-courbe hyperelliptique d'équation affine

$$\mathcal{D} : \nu^2 = (1-\mu^2)Q(-\mu^2).$$

L'application $\Gamma_{\mathcal{D}} : \begin{array}{ccc} k'(x)(\mathcal{C}) & \longrightarrow & k'(x)(\mathcal{D}) \\ A(y,z) & \longmapsto & A(i\mu, i\nu) \end{array}$ est un $k'(x)$-isomorphisme.

De plus, l'involution $\sigma_{\mathcal{D}} := \Gamma_{\mathcal{D}} \circ \sigma \circ \Gamma_{\mathcal{D}}^{-1}$ est donnée par $\sigma_{\mathcal{D}}(A(\mu,\nu)) = \sigma(A)(-\mu,-\nu)$ pour tout $A(\mu,\nu) \in k'(x)(\mathcal{D})$.

La $k(x)$-courbe $\mathcal{D}$ possède au moins deux points de ramification $k(x)$-rationnels : les points $(1,0)$ et $(-1,0)$.

Nous envoyons à l'infini un point de ramification $k'(x)$-rationnel de $\mathcal{C}$.

Plus précisément, nous envoyons le point $(1,0)$ à l'infini et le point $(-1,0)$ en $(0,0)$. Soit $\mathcal{H}$ la $k(x)$-courbe hyperelliptique d'équation affine $\beta^2 = h(\alpha)$ avec

$$h(\alpha) := -\alpha(\alpha-1)^{2g} Q\left(-\left(\frac{\alpha+1}{\alpha-1}\right)^2\right) \in k(x)[S].$$

Nous considérons $\mathcal{H}$ comme un revêtement de degré 2 de $\mathbb{P}^1_{k(x)}$. Il existe une homographie de $\mathbb{P}^1_{k(x)}$ qui envoie 1 en l'infini, -1 en 0 et le point à l'infini en 1. Elle induit un isomorphisme $\Gamma_{\mathcal{H}} : \begin{array}{ccc} k(x)(\mathcal{D}) & \longrightarrow & k(x)(\mathcal{H}) \\ A(\mu,\nu) & \longmapsto & A\left(\frac{\alpha+1}{\alpha-1}, \frac{2\beta}{(\alpha-1)^{g+1}}\right) \end{array}$

d'inverse $\begin{array}{ccc} k(x)(\mathcal{H}) & \longrightarrow & k(x)(\mathcal{D}) \\ A(\alpha,\beta) & \mapsto & A\left(\frac{\mu+1}{\mu-1}, \frac{2^g\nu}{(\mu-1)^{g+1}}\right) \end{array}$.

Ainsi l'involution $\sigma_{\mathcal{H}} := \Gamma_{\mathcal{H}} \circ \sigma_{\mathcal{D}} \circ \Gamma_{\mathcal{H}}^{-1}$ est définie pour tout $A(\alpha,\beta) \in k'(x)(\mathcal{H})$ par $\sigma_{\mathcal{H}}(A(\alpha,\beta)) = \sigma(A)\left(\frac{1}{\alpha}, \frac{(-1)^g\beta}{\alpha^{g+1}}\right)$.

Remarque :

L'action de $\sigma_{\mathcal{D}}$ sur $\mathcal{D}$ échange les points $(1,0)$ et $(-1,0)$. L'image de $(1,0)$ par $\Gamma_{\mathcal{H}}$ a été choisie telle que $\sigma_{\mathcal{H}}$ sur $\mathcal{H}$ échange le point à l'infini et le point $(0,0)$.

Nous normalisons.

Le polynôme h n'est en général pas unitaire. En fait, si nous écrivons $Q(T) = \sum_{l=0}^{g} Q_l T^l$ alors $h(\alpha) = -\alpha \sum_{l=0}^{g} (-1)^l Q_l (\alpha+1)^{2l} (\alpha-1)^{2(g-l)}$ est de coefficient dominant $-\sum_{l=0}^{g}((-1)^l Q_l) = -Q(-1)$. Nous posons $d := -Q(-1)$. Nous désignons par f_i le coefficient devant α^{i+1} dans $h(\alpha)$.

Nous utilisons une homothétie afin de nous ramener au cas unitaire : nous posons $s = d\alpha$ et $t = d^g\beta$. Nous avons ainsi un isomorphisme $\Gamma_{\widetilde{\mathcal{C}}}$ entre

$\mathcal{H}$ et la courbe $\widetilde{\mathcal{C}}$ d'équation $t^2 = f(s)$ où

$$\begin{aligned} f(s) &= \tfrac{s}{-d}(s-d)^{2g} Q\left(-\left(\tfrac{s+d}{s-d}\right)^2\right) \\ &= s(s^{2g} - f_{2g-1}s^{2g-1} - f_{2g-2}ds^{2g-2} - \cdots - f_0 d^{2g-1}). \end{aligned}$$

L'involution $\tau := \Gamma_{\widetilde{\mathcal{C}}} \circ \sigma_{\mathcal{H}} \circ \Gamma_{\widetilde{\mathcal{C}}}^{-1}$ est donnée par $\tau(A(s,t)) = \sigma(A)(\frac{d^2}{s}, (-1)^g \frac{d^{g+1}t}{s^{g+1}})$ pour tout $A(s,t) \in k'(x)(\widetilde{\mathcal{C}})$.

Théorème 2.1.1 *Soit k un sous-corps de $\mathbb{R}$. Nous notons $k' := k(i)$ et $Gal(k'/k) = \{1, \sigma\}$. Soient $Q \in k(x)[T]$ un polynôme tel que le polynôme $(y^2+1)Q(y^2)$ soit sans facteur carré. Soit $\mathcal{C}$ la courbe hyperelliptique sur $k(x)$ d'équation affine $z^2 + (y^2+1)Q(y^2) = 0$. Soient g le degré de Q et $d = -Q(-1) \in k(x)$. Nous supposons d non nul. Soit $\widetilde{\mathcal{C}}$ la courbe hyperelliptique sur $k(x)$ d'équation affine $t^2 = \frac{s}{-d}(s-d)^{2g} Q\left(-\left(\frac{s+d}{s-d}\right)^2\right)$.*

Alors, l'application $\Gamma : \begin{array}{ccc} k'(x)(\mathcal{C}) & \longrightarrow & k'(x)(\widetilde{\mathcal{C}}) \\ A(y,z) & \longmapsto & A(i\frac{s+d}{s-d}, \frac{2idt}{(s-d)^{g+1}}) \end{array}$ *est un $k'(x)$-isomorphisme d'inverse* $\Gamma^{-1} : \begin{array}{ccc} k'(x)(\widetilde{\mathcal{C}}) & \longrightarrow & k'(x)(\mathcal{C}) \\ A(s,t) & \longmapsto & A(d\frac{y+i}{y-i}, \frac{2^g d^g i^g z}{(y-i)^{g+1}}) \end{array}$.

De plus, l'involution $\tau := \Gamma \circ \sigma \circ \Gamma^{-1}$ envoie un élément $A(s,t) \in k'(x)(\widetilde{\mathcal{C}})$, sur $\tau(A) = \sigma(A)(\frac{d^2}{s}, (-1)^g \frac{d^{g+1}t}{s^{g+1}})$. En particulier, τ commute à l'involution hyperelliptique de $\widetilde{\mathcal{C}}$.

Définition 2.1.2 *Nous conservons les notations et hypothèses du théorème 2.1.1. Nous supposons $k = \mathbb{R}$.*

Un point $\alpha \in Jac(\widetilde{\mathcal{C}})(\mathbb{C}(x))^\tau = Pic^0(\mathbb{C}(x)(\widetilde{\mathcal{C}}))^\tau$ (le groupe des éléments τ-invariants de $Jac(\widetilde{\mathcal{C}})(\mathbb{C}(x))$) est dit τ-antineutre s'il existe un représentant $D \in Div(\mathbb{C}(x)(\widetilde{\mathcal{C}}))$ de la classe d'équivalence linéaire α et une fonction $h \in \mathbb{C}(x)(\mathcal{C})$ tels que :

* *$\tau(D) - D = div(h)$ et*
* *$-h\tau(h) \in \boxed{2}_{\mathbb{R}(x)}$ (le groupe multiplicatif des sommes non nulles de 2 carrés de $\mathbb{R}(x)$).*

Corollaire 2.1.3 *Nous conservons les notations et hypothèses du théorème 2.1.1. Nous supposons $k = \mathbb{R}$. L'isomorphisme Γ induit alors un isomorphisme*

$$\widetilde{\Gamma} : Jac(\mathcal{C} \times_{\mathbb{R}(x)} \mathbb{C}(x)) \longrightarrow Jac(\widetilde{\mathcal{C}} \times_{\mathbb{R}(x)} \mathbb{C}(x))$$

tel que $\widetilde{\Gamma}(Jac(\mathcal{C})(\mathbb{R}(x))) = Jac(\widetilde{\mathcal{C}})(\mathbb{C}(x))^\tau$.

De plus, un élément $\alpha \in Jac(\mathcal{C})(\mathbb{R}(x))$ est antineutre si et seulement si $\widetilde{\Gamma}(\alpha)$ est τ-antineutre.

Remarque :

Nous reprenons les notations 1.2.3 (appliquées au cas $\mathcal{D} := \mathcal{C}$). Nous posons
$\widetilde{\varpi} = \varpi \circ \widetilde{\Gamma}^{-1}$. La seconde assertion est seulement une traduction du fait qu'un point $\alpha \in \mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))^{\tau}$ est τ-antineutre si et seulement si $\widetilde{\varpi}(\alpha)$ est la classe de -1 : avec les notations de la définition 2.1.2, nous avons $h\tau(h) = \widetilde{\Gamma}^{-1}(h)\sigma(\widetilde{\Gamma}^{-1}(h)) = \widetilde{\varpi}(\alpha)$.

2.2 Comment déterminer les points antineutres de la jacobienne ?

Notations 2.2.1 Nous notons $\Sigma = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$. Soit $\boxed{2}_{\mathbb{R}(x)}$ le groupe multiplicatif des sommes non nulles de deux carrés dans $\mathbb{R}(x)$.

Soient $Q(Y) \in \mathbb{R}(x)[Y]$ et $P(Y) := (Y^2+1)Q(Y^2)$. Nous supposons le polynôme P totalement positif, unitaire, sans facteur carré, de degré strictement positif multiple de 4.

Soient g le degré de Q et $d = -Q(-1) \in \mathbb{R}(x)$. Nous supposons d non nul. Soit $f(s) := \frac{s}{-d}(s-d)^{2g}Q\left(-\left(\frac{s+d}{s-d}\right)^2\right)$. Soit $\widetilde{\mathcal{C}}$ la courbe hyperelliptique sur $\mathbb{R}(x)$ d'équation affine $t^2 = f(s)$, c'est-à-dire

$$\widetilde{\mathcal{C}} : t^2 = \frac{s}{-d}(s-d)^{2g}Q\left(-\left(\frac{s+d}{s-d}\right)^2\right).$$

Nous notons τ l'involution de $\mathbb{C}(x)(\widetilde{\mathcal{C}})$ qui envoie un élément $A(s,t) \in \mathbb{C}(x)(\widetilde{\mathcal{C}})$, sur $\tau(A) = \sigma(A)(\frac{d^2}{s}, -\frac{d^{g+1}t}{s^{g+1}})$ (ici, g est impair donc $(-1)^g = -1$).

Nous notons ∞ la place de $\mathbb{C}(x)(\widetilde{\mathcal{C}})$ au-dessus de la place à l'infini de $\mathbb{C}(x)(s)$ et $\mathcal{P}_0$ la place de $\mathbb{C}(x)(\widetilde{\mathcal{C}})$ d'abscisse 0.

Proposition 2.2.2 *Nous conservons les notations 2.2.1.*

Soit $D = div(u,v) \in Div^0(\mathbb{C}(x)(\widetilde{\mathcal{C}}))$ un diviseur réduit de poids m. Nous supposons que $\mathcal{P}_0 \notin Supp(D)$. Soit e le quotient de la division euclidienne de $m+1 = \deg_s(u)+1$ par 2.

Alors le diviseur $\tau(D) + div(s^e)$ est semi-réduit et $\tau(D) + div(s^e) = div\left(\frac{1}{u(0)}s^{2e}u\left(\frac{d^2}{s}\right), \hat{v}\right)$ avec $\hat{v}$ le reste de la division euclidienne de $-\left(\frac{s}{d}\right)^{g+1}v(\frac{d^2}{s})$ par $s^{2e}u(\frac{d^2}{s})$.

Démonstration.

Nous écrivons $D = \left(\sum_{i=1}^{r} n_i\mathcal{P}_i\right) - m\infty$ avec $\mathcal{P}_i$ des places de $\mathbb{C}(x)(\widetilde{\mathcal{C}})$ différentes de ∞ et $n_i \in \mathbb{N}$. Nous calculons alors $\tau(D)$ à l'aide de l'égalité

$\tau(\infty) = \mathcal{P}_0$. Nous obtenons

$$\begin{aligned}\tau(D) &= \left(\sum_{i=1}^{r} n_i \tau(\mathcal{P}_i)\right) - m\mathcal{P}_0 \\ &= \left(\left(\sum_{i=1}^{r} n_i \tau(\mathcal{P}_i)\right) - m\infty\right) - m(\mathcal{P}_0 - \infty).\end{aligned}$$

Ce diviseur n'est pas semi-réduit : sa valuation en $\mathcal{P}_0$ est négative. Pour résoudre cette difficulté, nous considérons le diviseur principal $\mathrm{div}(s) = 2\mathcal{P}_0 - 2\infty$. Par définition de e, nous avons $m \leq 2e \leq m+1$. Par conséquent, $v_{\mathcal{P}_0}(\tau(D) + \mathrm{div}(s^e))$ est égale à 0 ou 1.

Par ailleurs, τ commute à l'involution hyperelliptique et D est un diviseur semi-réduit, donc $\tau(D) + \mathrm{div}(s^e)$ est semi-réduit. Nous notons (u_τ, v_τ) la représentation de Mumford de $\tau(D) + \mathrm{div}(s^e)$.

Nous reprenons les notations de la proposition 1.4.2. L'idéal de $\mathbb{C}(x)[\mathcal{C}]$ associé à $\tau(D) + \mathrm{div}(s^e)$ est

$$\begin{aligned}I &:= \Upsilon(\tau(D) + \mathrm{div}(s^e)) \\ &= \left(\prod_{i=1}^{r} \left(\tau(\mathcal{P}_i) \bigcap \mathbb{C}(x)[\mathcal{C}]\right)^{n_i}\right) . (\mathcal{P}_0 \bigcap \mathbb{C}(x)[\mathcal{C}])^{2e-m} \\ &= \left(\bigcap_{i=1}^{r} \tau(\mathcal{P}_i)^{n_i}\right) \bigcap \mathcal{P}_0^{2e-m} \bigcap \mathbb{C}(x)[\mathcal{C}].\end{aligned}$$

De l'égalité $\mathrm{div}(s) = 2(\mathcal{P}_0 - \infty)$ nous déduisons que, pour tout $h \in \mathbb{C}(x)(\mathcal{C})$ et tout $r \in \mathbb{Z}$,

$$v_{\mathcal{P}}(s^r \tau(h)) = \begin{cases} v_{\mathcal{P}}(\tau(h)) = v_{\tau^{-1}(\mathcal{P})}(h) & \text{si } \mathcal{P} \notin \{\mathcal{P}_0, \infty\} \\ 2r + v_{\mathcal{P}_0}(\tau(h)) = 2r + v_\infty(h) & \text{si } \mathcal{P} = \mathcal{P}_0. \end{cases} \tag{2.1}$$

Nous appliquons les égalités 2.1 au cas $h = u$ et $r = 2e$: puisque

* $v_{\mathcal{P}_i}(u) \geq n_i$ si $i \neq 0$,
* $v_{\mathcal{P}}(u) \geq 0$ si $\mathcal{P} \neq \infty$,
* $v_\infty(u) = -2\deg_s(u)$ (car $v_\infty(s) = -2$) et donc $v_\infty(u) = -2m$ (d'après le lemme 1.4.8),

le polynôme $s^{2e}\tau(u) = s^{2e} u\left(\frac{d^2}{s}\right)$ appartient à l'idéal

$$\left(\bigcap_{i=1}^{r} \tau(\mathcal{P}_i)^{n_i}\right) \bigcap \mathcal{P}_0^{2(2e-m)} \bigcap \mathbb{C}(x)[\mathcal{C}] \subset I.$$

Le diviseur D est réduit donc $\deg_s(v) < g$. Ainsi, D'après le lemme 1.4.5 et la proposition 1.4.8, nous avons

$$v_\infty(t - v) = v_\infty(\mathrm{div}(t - v)) = -\deg_s(v^2 - f) = -2g - 1.$$

Par conséquent, en posant $h = t - v$ et $r = g + 1$ dans les égalités 2.1, nous montrons que $s^{g+1}\tau(t - v) = -d^{g+1}t + s^{g+1}v\left(\frac{d^2}{s}\right)$ appartient à I.

Soit J l'idéal de $\mathbb{C}(x)[\mathcal{C}]$ engendré par $s^{2e}u\left(\frac{d^2}{s}\right)$ et $t - \hat{v}$. Nous venons de montrer que $J \subset I$.

Nous notons (u_τ, v_τ) la représentation de Mumford de $\tau(D) + \mathrm{div}(s^e)$. D'après le lemme 1.4.5, u_τ engendre $N_{\mathbb{C}(x)(\mathcal{C})/\mathbb{C}(x)(s)}(I)$ et $s^{2e}u\left(\frac{d^2}{s}\right)$ engendre $N_{\mathbb{C}(x)(\mathcal{C})/\mathbb{C}(x)(s)}(J)$. Comme $J \subset I$, l'idéal $N_{\mathbb{C}(x)(\mathcal{C})/\mathbb{C}(x)(s)}(I)$ contient $N_{\mathbb{C}(x)(\mathcal{C})/\mathbb{C}(x)(s)}(J)$ et donc $s^{2e}u\left(\frac{d^2}{s}\right)$. Le polynôme u_τ divise donc $s^{2e}u\left(\frac{d^2}{s}\right)$.

Comme u ne s'annule pas en 0, le degré de $s^{2e}u\left(\frac{d^2}{s}\right)$ est $2e$. D'après la proposition 1.4.8, le degré de u_τ est le poids de $\tau(D) + \mathrm{div}(s^e)$. Or $v_\infty(\tau(D)) = v_{\tau^{-1}(\infty)}(D) = v_{\mathcal{P}_0}(D) = 0$, donc le degré de u_τ est $2e$. Les polynômes u_τ et $\frac{s^{2e}}{u(0)}u\left(\frac{d^2}{s}\right)$ sont unitaires de même degrés et $u_\tau | \frac{s^{2e}}{u(0)}u\left(\frac{d^2}{s}\right)$, donc $u_\tau = \frac{s^{2e}}{u(0)}u\left(\frac{d^2}{s}\right)$.

Soit $w := v_\tau - \hat{v} = (t - \hat{v}) - (t - v) \in I$. L'idéal engendré par w et $t - v_\tau$ est contenu dans I. D'après le lemme 1.4.5, w est soit nul soit un générateur de $N_{\mathbb{C}(x)(\mathcal{C})/\mathbb{C}(x)(s)}((w, t - v_\tau)) \subset N_{\mathbb{C}(x)(\mathcal{C})/\mathbb{C}(x)(s)}(I) = (u_\tau)$. Ainsi, w est soit nul soit divisible par u_τ. Le deuxième cas est exclu puisque v_τ et $\hat{v}$ sont de degrés strictement inférieurs à $\deg_s(u_\tau)$. Par suite, $w = v_\tau - \hat{v}$ est nul et donc $v_\tau = \hat{v}$.

Nous avons ainsi montré les égalités

$$u_\tau = \frac{s^{2e}}{u(0)}u\left(\frac{d^2}{s}\right) \text{ et } v_\tau = \hat{v}.$$

Pour conclure, nous utilisons la définition de u_τ et v_τ : le diviseur $\tau(D) + \mathrm{div}(s^e)$ est le diviseur semi-réduit de représentation de Mumford (u_τ, v_τ). □

Lemme 2.2.3 *Nous conservons les notations 2.2.1. Soient u, v_1, $v_2 \in \mathbb{C}(x)[s]$ trois polynômes. Soit $e \in \mathbb{N}$ un entier tel que $\deg_s(v_1) \leq e$ et $\deg_s(v_2) \leq e$.*

Nous avons alors équivalence entre :

* $v_1 \equiv v_2 \bmod u$, *et*
* $s^e\tau(v_1) \equiv s^e\tau(v_2) \bmod \left(s^{\deg_s(u)}\tau(u)\right)$.

Démonstration.

1. Supposons que $v_1 \equiv v_2 \bmod u$. Il existe alors un polynôme $q \in \mathbb{C}(x)[s]$ tel que $v_1 = v_2 + qu$. En appliquant τ à cette dernière égalité puis en multipliant par s^e, nous obtenons :

$$s^e\tau(v_1) = s^e\tau(v_2) + s^{e-\deg_s(u)}\tau(q)s^{\deg_s(u)}\tau(u). \tag{2.2}$$

La fraction rationnelle $s^{e-\deg_s(u)}\tau(q)$ est en fait un élément de $\mathbb{C}(x)[s]$ car

$$\begin{aligned}\deg_s(q)+\deg_s(u) &= \deg_s(v_1-v_2)\\ &\leq \max(\deg_s(v_1),\deg_s(v_2))\leq r.\end{aligned}$$

Ainsi l'égalité 2.2 implique la congruence $s^e\tau(v_1)\equiv s^e\tau(v_2) \bmod \left(s^{\deg_s(u)}\tau(u)\right)$.

2. Supposons maintenant que $s^e\tau(v_1)\equiv s^e\tau(v_2) \bmod \left(s^{\deg_s(u)}\tau(u)\right)$. Puisque $\deg_s(s^e\tau(v_1))=e-\deg_s(v_1)\leq e$ et $\deg_s(s^e\tau(v_2))=e-\deg_s(v_2)\leq e$, nous pouvons appliquer le raisonnement du point 1 en remplaçant v_1 par $s^e\tau(v_1)$ et v_2 par $s^e\tau(v_2)$. Ainsi, τ étant une involution, nous obtenons

$$d^{2e}v_1\equiv d^{2e}v_2 \bmod \left(d^{\deg_s(u)}u\right),$$

c'est-à-dire $v_1\equiv v_2 \bmod u$. $\square$

Théorème 2.2.4 *Nous conservons les notations 2.2.1.*

Soit $\alpha =< u,v >$ un élément de $Jac(\widetilde{\mathcal{C}})(\mathbb{C}(x))$ tel que $\mathcal{P}_0\notin Supp(\alpha)$ (i.e. tel que $u(0)$ soit non nul). Nous désignons par $\check{v}$ l'unique polynôme de degré inférieur ou égal à $deg(u)$, s'annulant en 0 et congru à v modulo u.
Alors α est τ-invariant si et seulement si :

* *$\deg_s(u)$ est pair, $s^{\deg_s(u)}\tau(u)=u(0)u(s)$ et le reste de la division euclidienne de $-\left(\frac{s}{d}\right)^{g+1}\tau(v)$ par u est v, ou*
* *u est de degré g et $\left(\frac{s}{d}\right)^{g+1}\tau(\check{v})=\check{v}$ et $u(0)(f-\check{v}^2)=su(s)s^g\tau(u(s))$.*

Si α est τ-invariant de poids strictement inférieur à g, alors pour tout point $\beta\in Jac(\widetilde{\mathcal{C}})(\mathbb{C}(x))$ nous avons équivalence entre :

* *β est τ-antineutre et*
* *$\alpha+\beta$ est τ-antineutre.*

Si α est τ-invariant de poids g, alors nous avons équivalence entre

* *α est τ-antineutre et*
* *$u(0)$ est une somme non nulle de carrés.*

De plus, si α est τ-antineutre, alors $-d^{g-1}=u(0)h\tau(h)$ avec $h=\frac{t+\check{v}}{su(s)}$.

Démonstration.

Nous reprenons les notations 1.2.3 (appliquées au cas $\mathcal{D}:=\mathcal{C}$). Nous posons $\widetilde{\varpi}:=\varpi\circ\widetilde{\Gamma}^{-1}$.

Soit e le quotient de la division euclidienne de $\deg_s(u)+1$ par 2 et soit ϵ le reste. Nous notons $D:=\mathrm{div}(u,v)$.

Soit $\hat{v}$ le reste de la division euclidienne de $-\left(\frac{s}{d}\right)^{g+1}v\left(\frac{d^2}{s}\right)$ par $s^{\deg_s(u)}u\left(\frac{d^2}{s}\right)$. Le polynôme $\frac{s^{deg_s(u)}}{u(0)}u\left(\frac{d^2}{s}\right)$ est unitaire. Nous notons $\widehat{D}:=\mathrm{div}\left(\frac{s^{deg_s(u)}}{u(0)}u\left(\frac{d^2}{s}\right),\hat{v}\right)$.

D'après la proposition 2.2.2, le point α est τ-invariant si et seulement si le diviseur

$$\begin{aligned}\tau(D) - D &= \widehat{D} + (1-\epsilon)(\mathcal{P}_0 - \infty) - \mathrm{div}(s^e) - D \\ &= \widehat{D} - (D + (1-\epsilon)(\mathcal{P}_0 - \infty)) + 2(1-\epsilon)(\mathcal{P}_0 - \infty) - \mathrm{div}(s^e) \\ &= \widehat{D} - (D + (1-\epsilon)(\mathcal{P}_0 - \infty)) - \mathrm{div}(s^{e-1+\epsilon})\end{aligned}$$

est principal. Nous sommes amenés à distinguer trois cas (suivant le degré de u).

Si $\deg_s(u)$ est impair et inférieur à $g-1$: les diviseurs $\widehat{D}$ et $D + (\mathcal{P}_0 - \infty) = \mathrm{div}\,(su(s), \check{v})$ sont réduits et leurs poids sont de parités distinctes. Ces deux diviseurs ne peuvent donc être linéairement équivalents. Comme $\epsilon = 0$, le diviseur $\tau(D) - D$ n'est pas principal.

Si $\deg_s(u)$ est pair : alors $\epsilon = 1$ et les diviseurs D et $\widehat{D}$ sont réduits. Par conséquent, le diviseur $\tau(D) - D$ est principal si et seulement si $D = \widehat{D}$, c'est-à-dire si et seulement si $u(0)u(s) = s^{deg_s(u)} u\left(\frac{d^2}{s}\right)$ et $v = \hat{v}$. Dans ce cas, le diviseur $\tau(D) - D$ est le diviseur principal associé à la fonction $h := s^{-e}$. Comme $h\tau(h) = d^{-2e}$, l'image $\widetilde{\varpi}(\alpha)$ est triviale. Or $\widetilde{\varpi}$ est un morphisme, donc, pour tout point $\beta \in \mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))$, nous avons équivalence entre :

* β est τ-antineutre et
* $\alpha + \beta$ est τ-antineutre.

Si u est de degré g : le polynôme $\check{v}$ est de degré strictement inférieur à $\deg_s(su(s)) = g+1$. Par suite, le polynôme $\frac{f-\check{v}^2}{su(s)}$ est unitaire : le polynôme f est unitaire et

$$2\deg_s(\check{v}) \leq 2g < 2g+1 = \deg_s(f).$$

Ainsi, comme $f - \check{v}^2 = (t - \check{v})(t + \check{v})$, nous avons

$$\mathrm{div}(t + \check{v}) = \mathrm{div}\left(f - \check{v}^2, -\check{v}\right).$$

Puisque u est de degré g, nous avons $\epsilon = 0$. Nous appliquons l'algorithme de réduction de Cantor au diviseur $D + \mathcal{P}_0 - \infty = \mathrm{div}(su(s), \check{v})$. Le diviseur $\mathrm{div}(su(s), \check{v})$ est de poids $g+1$. L'algorithme de réduction de Cantor s'achève donc au bout d'une itération. Cette itération s'obtient en écrivant l'égalité

$$\mathrm{div}(t + \check{v}) = \mathrm{div}\left(f - \check{v}^2, -\check{v}\right) = \mathrm{div}(su(s), -\check{v}) + \mathrm{div}(\widetilde{u}, \widetilde{v}) \tag{2.3}$$

avec $\widetilde{u} = \frac{f-\check{v}^2}{su(s)}$ et $\widetilde{v}$ le reste de la division euclidienne de $-\check{v}$ par $\widetilde{u}$ (c.f. la proposition 1.4.7, assertion 2, pour une preuve de ces égalités).

Nous appliquons maintenant la proposition 1.4.7, assertion 1 : nous avons

$$\begin{aligned}-\mathrm{div}(su(s), -\check{v}) &= \mathrm{div}(su(s), \check{v}) - \mathrm{div}(su(s)) \\ &= \mathrm{div}(su(s), \check{v}) + \mathrm{div}\left(\tfrac{1}{su(s)}\right).\end{aligned}$$

Ainsi, nous pouvons reformuler les égalités 2.3 sous la forme

$$\mathrm{div}\left(\frac{t+\check{v}}{su(s)}\right) + \mathrm{div}(su(s), \check{v}) = \mathrm{div}(\widetilde{u}, \widetilde{v})$$

Puisque les diviseurs $\widehat{D}$ et $\mathrm{div}(\widetilde{u}, \widetilde{v})$ sont réduits, le diviseur

$$\begin{array}{rcl} \tau(D) - D & = & \widehat{D} - (D + P_0 - \infty) - \mathrm{div}(s^{e-1}) \\ & = & \widehat{D} - \mathrm{div}(\widetilde{u}, \widetilde{v}) - \mathrm{div}(s^{e-1}) + \mathrm{div}(\frac{t+\check{v}}{su(s)}). \end{array} \tag{2.4}$$

est principal si et seulement si $\widehat{D} = \mathrm{div}(\widetilde{u}, \widetilde{v})$. Ainsi, par unicité de la représentation de Mumford d'un diviseur, le diviseur $\tau(D) - D$ est principal si et seulement si les deux conditions suivantes sont vérifiées :

1. $\frac{1}{u(0)} s^{deg_s(u)} \sigma(u)\left(\frac{d^2}{s}\right) = \frac{f-\check{v}^2}{su(s)}$ et
2. $-\left(\frac{s}{d}\right)^{g+1} \tau(v) \equiv -\check{v} \bmod \widetilde{u}$.

Les degrés $\deg_s(\widetilde{u}) = \deg_s(f - \check{v}^2) - \deg_s(su(s)) = 2g + 1 - (g + 1)$ et $\deg_s(u) = g$ sont égaux. Ainsi, après application de τ à chacun de ses membres, la condition 1 se réécrit

$$\frac{d^{2\deg_s(u)}}{\sigma(u(0))} u = s^{\deg_s(\widetilde{u})} \tau(\widetilde{u}).$$

De plus, les polynômes $-\left(\frac{s}{d}\right)^{g+1} \tau(v)$ et $-\check{v}$ sont de degrés inférieurs ou égaux à $g+1$. Ainsi, d'après la proposition 2.2.3, la condition 2 est satisfaite si et seulement si $v \equiv \left(\frac{s}{d}\right)^{g+1} \tau(\check{v}) \bmod u$.

Le polynôme $\check{v}$ étant de degré au plus g, le polynôme $\left(\frac{s}{d}\right)^{g+1} \tau(\check{v})$ s'annule en 0. La condition 2 se reformule donc finalement sous la forme $\check{v} = \left(\frac{s}{d}\right)^{g+1} \tau(\check{v})$.

Lorsque α est un point τ-invariant de poids g de $\mathrm{Jac}(\widetilde{\mathcal{C}})$, l'égalité 2.4 signifie que $\tau(D) - D$ est le diviseur principal associé à la fonction $\frac{t+\check{v}}{s^e u(s)}$. Par conséquent, $\widetilde{\varpi}(\alpha)$ est la classe de $h\tau(h)$ avec $h = \frac{t+\check{v}}{s^e u(s)}$. Par τ-invariance de α, nous avons $\frac{s^{g+1}}{d^{g+1}} \tau(\check{v}) = \check{v}$. Or $g + 1 = 2e$, donc

$$\tau(h) = \frac{s^e\left(-\frac{d^{g+1}}{s^{g+1}} t + \tau(\check{v})(s)\right)}{d^{2e}\tau(u)(s)} = -\frac{s^e(t - \check{v})}{s^{g+1}\tau(u)(s)},$$

et nous pouvons donc écrire

$$h\tau(h) = -\frac{t^2 - \check{v}^2}{su(s)s^g\tau(u(s))} = -\frac{f - \check{v}^2}{su(s)s^g\tau(u(s))}.$$

Nous utilisons une nouvelle fois la τ-invariance de α : nous avons

$$su(s)s^g\tau(u(s)) = u(0)(f - \check{v}^2).$$

Ainsi $u(0)h\tau(h) = -1$, et $\widetilde{\varpi}(\alpha)$ est la classe de $-u(0)$.

La formule annoncée au cours de la proposition est

$$u(0)\widetilde{h}\tau(\widetilde{h}) = -d^{g-1}$$

avec $\widetilde{h} := \frac{t+\breve{v}}{su(s)} = s^{e-1}h$. Cette formule se démontre à partir de l'égalité $u(0)h\tau(h) = -1$ en remarquant l'égalité

$$s^{e-1}\tau(s^{e-1}) = d^{2e-2} = d^{g-1}. \quad \square$$

Remarque :

Nous conservons la notation $\widetilde{\varpi}$ introduite au début de la démonstration. Comme $\tau(< s, 0 >) - < s, 0 >= (s^{-1})$, l'image $\widetilde{\varpi}(< s, 0 >)$ est la classe de $s^{-1}\tau(s^{-1}) = d^{-2}$, c'est-à-dire la classe triviale.

Nous n'avons pas étudié la τ-antineutralité d'éléments de $\mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))$ de la forme $< su(s), v >$. Puisque $< s, 0 >$ est τ-invariant, $< u, v \bmod u >$ est τ-invariant si et seulement si $< su(s), v >$ est τ-invariant. Supposons que cela soit le cas. L'application $\widetilde{\varpi}$ est un morphisme :

$$\begin{aligned} \widetilde{\varpi}(< su(s), v(s) >) &= \widetilde{\varpi}(< s, 0 >).\widetilde{\varpi}(< u, v \bmod u >) \\ &= \widetilde{\varpi}(< u, v \bmod u >). \end{aligned}$$

De plus, $\widetilde{\varpi}(< u, v \bmod u >)$ est l'image d'un diviseur de degré au plus $g-1$ et est donc la classe triviale. Finalement l'image du diviseur $< su(s), v >$ est triviale et le diviseur $< su(s), v >$ ne peut en aucun cas être τ-antineutre.

2.3 Comment calculer la torsion 2-primaire ?

2.3.1 Comment diviser par 2 dans la jacobienne ?

Proposition 2.3.1.1 *Soit k un corps de caractéristique 0. Soient $f \in k[y]$ un polynôme de degré impair et $\mathcal{C}$ la courbe hyperelliptique d'équation affine $z^2 = f(y)$. Soit $div(u_0, v_0) \in Div^0(k(\mathcal{C}))$ un diviseur semi-réduit. Soit $w \in k[y]$ un polynôme sans facteur carré.*

Alors il existe un diviseur semi-réduit $div(u, v) \in Div^0(k(\mathcal{C}))$ linéairement équivalent à $div(u_0, v_0)$ tel que u et w soient premiers entre eux.

Démonstration.

Puisque l'addition dans $\mathrm{Div}^0(k(\mathcal{C}))$ est compatible à la relation d'équivalence linéaire, on peut supposer sans perte de généralité que u_0 est égal à un facteur premier p de w.

Soit $d := \mathrm{pgcd}\left(v_0^2 - f, \frac{w}{p}\right)$. Le polynôme w se factorise sous la forme $w = dw_1$.

Les polynômes d et w_1 étant premiers entre eux (w est sans facteur carré), w_1 est inversible modulo les facteurs premiers de d. Par conséquent,

il existe $\lambda \in k$ non nul tel que, pour tout facteur premier q de d, on ait $\lambda w_1 \not\equiv 2v_0 \bmod d$ (on peut déterminer un tel λ en utilisant par exemple le lemme chinois).

De plus, les polynômes $\frac{w_1}{p}$ et p étant premiers entre eux, $2\frac{w_1}{p}$ est inversible modulo p. On peut donc choisir λ de telle façon que $2\lambda\frac{w_1}{p} \not\equiv \frac{v_0^2-f}{p} \bmod p$.

On considère la fonction $h := y + v_0 - \lambda w_1$, et on note $u := \frac{N_{k(\mathcal{C})/k(y)}(h)}{p}$ et v le reste de la division euclidienne de $-v_0 + \lambda w_1$ par u. Le diviseur

$$\mathrm{div}(u, v) = \mathrm{div}(h) - \mathrm{div}(p, -v_0) = \mathrm{div}\left(\frac{h}{p}\right) + \mathrm{div}(p, v_0)$$

est bien linéairement équivalent à $\mathrm{div}(p, v_0)$.

Nous allons montrer que les polynômes w et $u = \frac{N_{k(\mathcal{C})/k(y)}(h)}{p}$ sont premiers entre eux. Soit q un facteur premier de w. Nous vérifions que q ne divise pas u en distinguant trois cas.

Si $q \neq p$ et $q|w_1$: comme q divise w_1, qui est premier à $v_0^2 - f$, le polynôme

$$N_{k(\mathcal{C})/k(y)}(h) = (-v_0 + \lambda w_1)^2 - f \equiv v_0^2 - f \bmod q.$$

n'est pas divisible par q.

Si $q|d$: comme
$$\begin{aligned} N_{k(\mathcal{C})/k(y)}(h) &= (-v_0 + \lambda w_1)^2 - f \\ &= v_0^2 - f - 2\lambda v_0 w_1 + \lambda^2 w_1^2 \\ &\equiv \lambda w_1(\lambda w_1 - 2v_0) \bmod q, \end{aligned}$$
et comme λ a été choisi tel que d et $\lambda w_1 - 2v_0$ soient premiers entre eux, le polynôme irréductible q ne divise pas $N_{k(\mathcal{C})/k(y)}(h)$.

Si $q = p$: par définition de λ, le polynôme irréductible p ne divise pas $\frac{v_0^2-f}{p} - 2\lambda v_0 \frac{w_1}{p}$. On en déduit que p n'est pas un facteur premier de

$$\begin{aligned} \frac{N_{k(\mathcal{C})/k(y)}(h)}{p} &= \frac{(v_0-\lambda w_1)^2-f}{p} \\ &= \frac{v_0^2-f}{p} - 2\lambda v_0 \frac{w_1}{p} + p\lambda^2 \left(\frac{w_1}{p}\right)^2. \end{aligned}$$ □

Soit k un corps de caractéristique 0. Soient $f \in k[y]$ un polynôme unitaire de degré impair et $\mathcal{C}$ la courbe hyperelliptique sur k d'équation affine $z^2 = f(y)$. Au cours de la section 1.5 nous avons rappelé comment définir un morphisme de noyau $2\mathrm{Jac}(\mathcal{C})(k)$. Le théorème suivant fournit une nouvelle caractérisation de $2\mathrm{Jac}(\mathcal{C})(k)$. Cette caractérisation a pour avantage d'être effective.

Théorème 2.3.1.2 *Soit k un corps de caractéristique* 0.

Soient $f \in k[y]$ un polynôme unitaire de degré impair et $\mathcal{C}$ la courbe hyperelliptique sur k d'équation affine $z^2 = f(y)$. Soit $< u, v > \in Jac(\mathcal{C})(k)$. On note $w := \frac{v^2 - f}{u} \in k[y]$.

Alors $< u, v > \in 2Jac(\mathcal{C})(k)$ si et seulement si il existe trois polynômes a, q, $u_1 \in k[y]$ tels que

$$(-1)^{\deg(u)} u_1^2 = a^2 w + 2qav + q^2 u \tag{2.5}$$

et que u_1 soit premier avec u.

Supposons que l'équation 2.5 ait une solution (a, q, u_1) avec a et u_1 premiers entre eux et u_1 unitaire. On pose

* *$d := pgcd(a, q, u_1)$,*
* *$\widetilde{a} := \frac{a}{d}$, $\widetilde{q} := \frac{q}{d}$, $\widetilde{u_1} := \frac{u_1}{d}$,*
* *$\widetilde{v}_1 \in k[y]$ l'unique polynôme vérifiant $\widetilde{a}\widetilde{v}_1 \equiv \widetilde{a}v + \widetilde{q}u \bmod \widetilde{u_1}$ et $deg_y(\widetilde{v}_1) < deg_y(\widetilde{u}_1)$.*

Alors la classe d'équivalence linéaire du diviseur $2div(\widetilde{u_1}, -\widetilde{v}_1)$ est $< u, v >$.

Démonstration.
Si $< u, v > \in 2\mathbf{Jac}(\mathcal{C})(k)$: alors il existe $\mathrm{div}(u_1, v_1) \in \mathrm{Div}^0(k(\mathcal{C}))$ et a, $b \in k[y]$ tel que

$$2\mathrm{div}(u_1, v_1) + \mathrm{div}(u, v) = \mathrm{div}(az - b). \tag{2.6}$$

En appliquant le lemme 2.3.1.1 au diviseur $\mathrm{div}(u_1, v_1)$, on se ramène au cas où u et u_1 sont premiers entre eux. En terme d'idéaux, l'égalité 2.6 s'écrit

$$(u_1, z - v_1)^2 (u, z - v) = (az - b).$$

En appliquant $N_{k(\mathcal{C})/k(x)}$ on obtient l'existence de $\lambda \in k$ tel que

$$\lambda u_1^2 u = b^2 - a^2 f. \tag{2.7}$$

En fait, comme u et u_1 sont unitaires, λ est le coefficient dominant de $b^2 - a^2 f$.

Supposons que $\deg(u)$ soit pair. Alors $b^2 - a^2 f$ est de degré pair. Or b^2 est de degré pair et $a^2 f$ est de degré impair, donc le monôme dominant de $b^2 - a^2 f$ est celui de b^2. Par suite, il existe $\widetilde{\lambda} \in k^\times$ tel que $\lambda = \widetilde{\lambda}^2$. Quitte à diviser a et b par $\widetilde{\lambda}$, nous pouvons donc supposer que $\lambda = 1 = (-1)^{\deg(u)}$.

Supposons que $\deg(u)$ soit impair. Alors $b^2 - a^2 f$ est de degré impair. Or b^2 est de degré pair et $a^2 f$ est de degré impair, donc le monôme dominant de $b^2 - a^2 f$ est celui de $-a^2 f$. Le polynôme f étant unitaire, il existe $\widetilde{\lambda} \in k^\times$ tel que $\lambda = -\widetilde{\lambda}^2$. Quitte à diviser a et b par $\widetilde{\lambda}$, nous pouvons donc supposer que $\lambda = -1 = (-1)^{\deg(u)}$.

Par ailleurs $az - b \in (u, z - v)$, donc $av - b$ appartient à $(u, z - v) \cap k[y]$. Comme $(\mathrm{pgcd}(u, av - b), z - v) = (u, z - v)$, l'unicité de la représentation

de Mumford impose à u et $\mathrm{pgcd}(u, av-b)$ d'être égaux : u divise $av-b$. Il existe donc $q \in k[y]$ tel que $b = av + qu$. L'égalité 2.7 s'écrit alors

$$(-1)^{\deg(u)} u_1^2 u = (av+qu)^2 - a^2 f$$

c'est-à dire

$$(-1)^{\deg(u)} u_1^2 u = a^2(v^2 - f) + 2qavu + q^2u^2.$$

En divisant par u, on retrouve l'équation 2.5.

Si l'équation 2.5 a une solution (a, q, u_1) avec u_1 premier à u : quitte à les diviser par $\mathrm{pgcd}(a, q, u_1)$, on peut supposer a, q et u_1 premiers entre eux dans leur ensemble. Soit p un facteur premier de a. En réduisant l'équation 2.5 modulo p on obtient

$$(-1)^{\deg(u)} u_1^2 \equiv q^2 u \bmod p. \tag{2.8}$$

Puisque u_1 et u sont premiers entre eux, le polynôme p ne divise pas u. De plus, les polynômes a, q et u_1 sont premiers entre eux dans leur ensemble. D'après la congruence 2.8, le polynôme p ne divise donc ni q ni u_1. Ainsi a et $u_1^2 u$ sont premiers entre eux, et il existe donc un unique polynôme v_1 avec $\deg_y(v_1) < \deg_y(u_1^2 u)$ tel que

$$av_1 \equiv (av+qu) \bmod (u_1^2 u).$$

L'idéal $(u_1^2 u, z - v_1)$ contient $az - (av+qu)$. Par ailleurs,

$$\begin{aligned}(-1)^{\deg(u)} u_1^2 u &= u(a^2 w + 2qav + q^2 u) \\ &= (av+qu)^2 - a^2 f \\ &= N_{k(\mathcal{C})/k(y)}(az - (av+qu))\end{aligned}$$

appartient à l'idéal I engendré par $az-(av+qu)$. Par suite $av+qu-av_1$ appartient à I (il est divisible par $u_1^2 u$), et donc

$$a(z-v_1) = (az-(av+qu)) + (av_1 - (av+qu)) \in I.$$

Or a est inversible modulo $u_1^2 u \in I$ donc $z - v_1 \in I$. Ainsi, l'idéal $(u_1^2 u, z - v_1)$ est engendré par $az-(av+qu)$. D'après la proposition 1.4.7, on a donc :

$$2\mathrm{div}(u_1, v_1) + \mathrm{div}(u, v) = \mathrm{div}(az - (av+qu))$$

c'est-à-dire que $2\mathrm{div}(u_1, -v_1)$ est linéairement équivalent à $\mathrm{div}(u, v)$. □

Remarque :

Dans le cas particulier où le diviseur $< u, v >$ est un point de 2-torsion, c'est-à-dire lorsque $u | f$ et $v = 0$, l'équation 2.5 est $(-1)^{\deg(u)} u_1^2 = a^2 w + q^2 u$. La condition de primalité relative de u_1 et u impose à a d'être non nulle. Par suite l'équation 2.5 se réécrit

$$(-1)^{\deg(u)} w = N_{K_{\left(T^2 + (-1)^{\deg(u)+1} u\right)}/k(y)} \left(\frac{q}{a} T + (-1)^{\deg(u)} \frac{u_1}{a} \right)$$

avec $K_{\left(T^2+(-1)^{\deg(u)+1}u\right)} := k(y)[T]/(T^2+(-1)^{\deg(u)+1}u)$. Lors de la section 2.5.1, nous utilisons la multiplicativité de $N_{K_{\left(T^2+(-1)^{\deg(u)+1}u\right)}/k(y)}$ pour résoudre l'équation 2.5.

2.3.2 L'algorithme de calcul de la torsion 2-primaire

Nous reprenons les notations et hypothèses du théorème 2.3.1.2. La 2-torsion de $\mathrm{Jac}(\mathcal{C})(k)$ est connue : elle est constituée des points $< u, 0 >$ avec $u \in k[y]$ un diviseur de degré au plus g de f. L'idée pour calculer la torsion 2-primaire est d'itérer la division par 2 tant que c'est possible.

On se place à l'étape r, c'est-à-dire que l'on suppose que $\mathrm{Jac}(\mathcal{C})(k)[2^r]$ a été calculée. On se donne un point $\alpha =< u, v >\in \mathrm{Jac}(\mathcal{C})(k)[2^r]$. On souhaite trouver un point $\beta \in \mathrm{Jac}(\mathcal{C})(k)$ tel que $2\beta = \alpha$. Pour cela nous utilisons le théorème 2.3.1.2.

Le point α n'est pas toujours un double dans $\mathrm{Jac}(\mathcal{C})(k)$. On commence donc par utiliser le morphisme de Cassels-Schaefer afin de vérifier que $\alpha \in 2\mathrm{Jac}(\mathcal{C})(k)$. Dans les sections 2.4 et 2.5, cette vérification est effectuée grâce à la proposition :

Proposition 2.3.2.1 *Soient k_0 un corps de caractéristique différente de 2, δ un élément de k_0 et k l'extension quadratique de k_0 définie par $k := k_0[U]/(U^2-\delta)$.*

Soit $g := \alpha U + \beta \in k$ avec $\alpha \in k_0$ non nul et $\beta \in k_0$. Alors g est un carré dans k si et seulement si il existe γ, $\eta \in k_0$ tels que $N_{k/k_0}(g) = \gamma^2$ et $\frac{\beta+\gamma}{2} = \eta^2$. De plus, s'il existe γ, $\eta \in k_0$ tels que $N_{k/k_0}(g) = \gamma^2$ et $\frac{\beta+\gamma}{2} = \eta^2$, alors $\eta \neq 0$ et

$$\left(\frac{\alpha}{2\eta}U + \eta\right)^2 = \alpha U + \beta. \tag{2.9}$$

Soit $\beta \in k_0$. Alors β est un carré dans k si et seulement si β ou $\delta\beta$ est un carré dans k_0. De plus, s'il existe η tel que $\delta\beta = \eta^2$, alors $\beta = (T^{-1}\eta)^2$.

Démonstration.

On veut donner des conditions sur α et β pour qu'il existe a, $b \in k_0$ tels que $(aU+b)^2 = \alpha U + \beta$ c'est à dire que l'on veut résoudre le système :

$$\left\{ \begin{array}{rcl} \alpha & = & 2ab \\ \beta & = & a^2\delta + b^2 \end{array} \right.$$

Nous commençons par nous placer dans le cas où $\alpha \neq 0$. La première équation nous dit que b doit être non nul et que $a = \frac{\alpha}{2b}$. En reportant dans la seconde équation, on voit qu'alors b doit être solution de l'équation $b^4 - \beta b^2 + \frac{\alpha^2\delta}{4}$. Ainsi g est un carré dans k si et seulement si le polynôme $(T^2-\frac{\beta}{2})^2 + \frac{\alpha^2\delta-\beta^2}{4} = (T^2-\frac{\beta}{2})^2 - \frac{N_{k/k_0}(g)}{4}$ a une racine non nulle dans k_0. Si η est une telle racine, alors $\gamma := 2\eta^2 - \beta \in k_0$ vérifie $N_{k/k_0}(g) = \gamma^2$

et $\frac{\beta+\gamma}{2} = \eta^2$. Inversement s'il existe γ, $\eta \in k_0$ tel que $N_{k/k_0}(g) = \gamma^2$ et $\frac{\beta+\gamma}{2} = \eta^2$, alors η est racine de $(T^2 - \frac{\beta}{2})^2 - \frac{N_{k/k_0}(g)}{4}$, et donc

* $\eta \neq 0$ (comme $\alpha \neq 0$, nous avons $N_{k/k_0}(g) \neq \beta^2$),
* et le carré de $\frac{\alpha}{2\eta}U + \eta$ est bien $\alpha U + \beta$.

Nous supposons maintenant que $\alpha = 0$. Dans ce cas $2ab$ doit être nul et alors $a = 0$ ou $b = 0$. Le cas $a = 0$ signifie que $\beta = b^2$. Le cas $b = 0$ signifie que $\beta = (Ta)^2 = \delta a^2$, c'est à dire que $\delta\beta$ est un carré dans k. □

Nous déterminons les points de torsion τ-antineutres en appliquant la méthode suivante. On vérifie d'abord la τ-antineutralité des points de 2-torsion. Lorsque la τ-antineutralité des éléments de $\mathrm{Jac}(\mathcal{C})(k)[2^r]$ a été vérifiée nous appliquons à tout $\alpha \in \mathrm{Jac}(\mathcal{C})(k)[2^r]$ l'algorithme suivant :

1. déterminer si l'image $\pi_{\mathcal{C}}(\alpha)$ de α par le morphisme de Cassels-Schaefer $\pi_{\mathcal{C}}$ est triviale ;
2. si $\pi_{\mathcal{C}}(\alpha) = 1$, trouver un élément $\beta \in \mathrm{Jac}(\mathcal{C})(k)$ tel que $2\beta = \alpha$ (en utilisant les théorèmes 2.3.1.2 et 2.3.2.1) ;
3. pour tout $T \in \mathrm{Jac}(\mathcal{C})(k)[2]$, étudier la τ-antineutralité de $T+\beta$ à l'aide du théorème 2.2.4.

Ce faisant nous déterminons les éléments de $\mathrm{Jac}(\mathcal{C})(k)[2^{r+1}]$. Nous pouvons alors passer à l'étape $r + 1$.

Application :

Nous considérons une famille $(P_i)_{i\in I} \in \mathbb{R}[x, y]^I$ de polynômes positifs ou nuls sur $\mathbb{R}^2$. Nous notons $\mathcal{C}_i$ la courbe hyperelliptique d'équation affine $z^2 + P_i(x, y) = 0$. En appliquant la méthode précédente à la jacobienne $\mathrm{Jac}(\mathcal{C}_i)$, nous pouvons trouver des sous-familles de $(P_i)_{i\in I}$ dont les éléments sont des sommes de trois carrés dans $\mathbb{R}(x, y)$.

Une telle démarche est effectuée au cours de la section 2.5 pour les polynômes de la forme $P_{a,b,c}(x, y) := (y^2+1)(y^2+a(x))(y^2+b(x))(y^2+c(x))$ où a, b, $c \in \mathbb{R}(x)$ sont trois fractions rationnelles positives ou nulle sur $\mathbb{R}$.

2.4 Les polynômes de la forme $(y^2 + 1)(y^2 + C)(y^4 + (1 + C)y^2 + B)$.

Notations 2.4.1 Soient B et C deux éléments de $\mathbb{R}(x)$. Nous supposons le polynôme $P(x, y) := (y^2+1)(y^2+C)(y^4+(1+C)y^2+B)$ sans facteur carré c'est-à-dire

* C différent de 0 et 1,
* B différent de 0 et $\frac{(1+C)^2}{4}$ (le discriminant de $(y^4 + (1 + C)y^2 + B)$ est $16B((1 + C)^2 - 4B)^2$).
* B différent de C (ainsi les polynômes $(y^2 + 1)(y^2 + C)$ et $(y^4 + (1 + C)y^2 + B)$ sont premiers entre eux)

Soit $\mathcal{C}$ la $\mathbb{R}(x)$-courbe hyperelliptique d'équation affine

$$\mathcal{C} : z^2 + (y^2+1)(y^2+C)(y^4+(1+C)y^2+B) = 0.$$

Soit J la jacobienne de la courbe $\mathcal{C}$.

Nous souhaitons montrer que $J(\mathbb{R}(x))$ ne contient pas d'élément de torsion antineutre. Pour cela nous utilisons le théorème 2.1.1. Ce faisant, nous introduisons de nouvelles notations.

Notations 2.4.2 Nous posons $d := (1-C)(B-C)$,

$$\begin{aligned} g_1(s) &= \tfrac{-(s+d)^2+(s-d)^2}{-4d} = s, \\ g_2(s) &= \tfrac{-(s+d)^2+C(s-d)^2}{C-1} \\ &= s^2 + 2(1+C)(B-C)s + (1-C)^2(B-C)^2 \text{ et} \\ g_3(s) &= \tfrac{(s+d)^4-(1+C)(s+d)^2(s-d)^2+B(s-d)^4}{B-C} \\ &= s^4 + 4(1-C)(1-B)s^3 + 2(1-C)^2(B-C)(4+3B+C)s^2 \\ &\quad +4(1-C)^3(B-C)^2(1-B)s + (1-C)^4(B-C)^4. \end{aligned}$$

D'après le théorème 2.1.1, la courbe $\mathcal{C}$ est birationnellement équivalente sur $\mathbb{C}(x)$ à la courbe $\widetilde{\mathcal{C}}$ d'équation affine

$$\widetilde{\mathcal{C}} : t^2 = f(s) \text{ avec } f(s) = g_1(s)g_2(s)g_3(s).$$

Soit $\widetilde{J}$ la jacobienne de la courbe $\widetilde{\mathcal{C}}$.

On note σ la conjugaison complexe et

$$\begin{array}{rccc} \tau : & \mathbb{C}(x)(\widetilde{\mathcal{C}}) & \longrightarrow & \mathbb{C}(x)(\widetilde{\mathcal{C}}) \\ & a(s)t+b(s) & \longmapsto & -\sigma(a)\left(\frac{d^2}{s}\right)\frac{d^4 t}{s^4} + \sigma(b)\left(\frac{d^2}{s}\right). \end{array}$$

Pour $i = 1, 2, 3$, on pose $k_i := \mathbb{C}(x)[T]/(g_i(T))$. Soient

$$\pi_{\widetilde{\mathcal{C}}} : \widetilde{J}(\mathbb{C}(x)) \longrightarrow k_1^\times/k_1^{\times 2} \times k_2/k_2^{\times 2} \times k_3/k_3^{\times 2}$$

le morphisme de Cassels-Schaefer associé à $\widetilde{J}(\mathbb{C}(x)$ et $\pi_{\widetilde{\mathcal{C}},i} : \widetilde{J}(\mathbb{C}(x)) \longrightarrow k_i/k_i^{\times 2}$ sa i-ème coordonnée. Si α est est la classe d'équivalence linéaire d'un diviseur semi-réduit $\mathrm{div}(u,v)$ avec u premier à g_i, alors $\pi_{\widetilde{\mathcal{C}},i}(\alpha)$ est la classe de $(-1)^{\deg(u)}u(T)$ dans $k_i/k_i^{\times 2}$.

Nous reformulons nos deux problèmes à l'aide du théorème 2.1.1 : nous voulons montrer que $\widetilde{J}(\mathbb{C}(x))^\tau$ ne contient pas d'élément de torsion 2-primaire antineutre.

Il nous faut tout d'abord calculer $\widetilde{J}(\mathbb{C}(x))[2]$. Cela revient à factoriser le polynôme $f(s)$, c'est-à-dire les polynômes $g_2(s)$ et $g_3(s)$.

Lemme 2.4.3 *Le polynôme $U^4-(1+C)U^2+B$ n'est un produit de deux polynômes de degré 2 que dans les deux cas suivants :*

* *$(1+C)^2-4B=\mu^2$ pour un certain $\mu\in\mathbb{C}(x)$ et alors la factorisation de $U^4-(1+C)U^2+B$ est*

$$U^4-(1+C)U^2+B=\left(U^2-\frac{(1+C)+\mu}{2}\right)\left(U^2-\frac{(1+C)-\mu}{2}\right);$$

* *Il existe μ, $\nu\in\mathbb{C}(x)$ tels que $B=\nu^2$ et $1+C+2\nu=\mu^2$. Dans ce cas la factorisation de $U^4-(1+C)U^2+B$ est*

$$U^4-(1+C)U^2+B=(U^2+\mu U+\nu)(U^2-\mu U+\nu).$$

Démonstration.

Soient α, β, γ, $\delta\in\mathbb{C}(x)$ vérifiant $(U^2+\alpha U+\beta)(U^2+\gamma U+\delta)=U^4-(1+C)U^2+B$, c'est-à-dire tels que

$$\alpha+\gamma=0,\ \beta+\delta+\alpha\gamma=-1-C,\ \alpha\delta+\gamma\beta=0 \text{ et } \beta\delta=B.$$

La première équation nous dit que $\gamma=-\alpha$. En remplaçant dans la troisième équation, on voit que $\alpha(\delta-\beta)=0$. On a donc deux possibilités : $\alpha=0$ et $\beta=\delta$.

Si $\alpha=0$: les équations définissant α, β, γ et δ sont $\alpha=\gamma=0$, $\delta=-1-C-\beta$ et $\beta^2+(1+C)\beta+B=0$. Cette dernière équation n'a de solution que si $(1+C)^2-4B=\mu^2$ pour un certain $\mu\in\mathbb{C}(x)$ et dans ce cas ses solutions sont $-\frac{1+C+\mu}{2}$ et $-\frac{1+C-\mu}{2}$. Le cas où $\alpha=0$ correspond au premier cas énoncé dans la proposition.

Si $\beta=\delta$: les équations sont alors : $\gamma=-\alpha$, $\delta=\beta$, $\beta^2=B$ et $2\beta-\alpha^2=-1-C$. Nous sommes dans le deuxième cas annoncé dans la proposition avec $\mu=\alpha$ et $\nu=\beta$. □

Proposition 2.4.4 *Nous conservons les notations 2.4.1 et 2.4.2. Nous supposons que B, C et $(1+C)^2-4B$ ne sont pas des carrés dans $\mathbb{C}(x)$.*

La 2-torsion de $\widetilde{J}(\mathbb{C}(x))$ est alors constituée de l'élément neutre et des trois points $<g_1,0>$, $<g_2,0>$ et $<g_1g_2,0>$.

Démonstration.

Tout d'abord remarquons que $U^4-(1+C)U^2+B$ est un polynôme en U^2. Si le polynôme $U^4-(1+C)U^2+B$ admet une racine α, alors $-\alpha$ est également racine de $U^4-(1+C)U^2+B$. Dans ce cas, $U^4-(1+C)U^2+B$ est un produit de deux polynômes de degré 2. Ainsi, le polynôme $U^4-(1+C)U^2+B$ est soit irréductible soit un produit de deux polynômes de degré 2. Nous déduisons donc du lemme 2.4.3) que le polynôme $U^4-(1+C)U^2+B$ est irréductible.

Supposons que $g_3(s)$ soit un produit de deux polynômes $P_1, P_2 \in \mathbb{C}(x)[s]$. Pour $i = 1$ ou 2, on pose $Q_i := \left(\frac{U-1}{2d}\right)^{\deg(P_i)} P_i\left(d\frac{U+1}{U-1}\right) \in \mathbb{C}(x)[U]$. Nous évaluons

$$g_3(s) = (s-d)^4 \left(\left(\frac{s+d}{s-d}\right)^4 - (1+C)\left(\frac{s+d}{s-d}\right)^2 + B \right)$$

en $s = d\frac{U+1}{U-1}$ en utilisant les égalités $U = \frac{s+d}{s-d}$ et $s - d = \frac{2d}{U-1}$. On obtient

$$U^4 - (1+C)U^2 + B = \left(\frac{U-1}{2d}\right)^4 g_3\left(d\frac{U+1}{U-1}\right) = Q_1(U)Q_2(U).$$

Puisque $U^4-(1+C)U^2+B$ est irréductible, Q_1 ou Q_2 doit être constant et donc P_1 ou P_2 est être constant. Nous avons ainsi montré que $g_3(s)$ est irréductible.

Par ailleurs, C n'étant pas un carré dans $\mathbb{C}(x)$, le polynôme

$$\begin{array}{rcl} g_2(s) & = & s^2 - 2(1+C)(B-C)s + (1-C)^2(B-C)^2 \\ & = & (s-(1+C)(B-C))^2 - 4C(B-C)^2 \end{array}$$

n'a pas de racine dans $\mathbb{C}(x)$ et est donc irréductible sur $\mathbb{C}(x)$. Pour conclure il suffit de rappeler que $\widetilde{J}(\mathbb{C}(x))[2]$ est l'ensemble des points de représentations de Mumford $< u(s), 0 >$ avec $u(s) \in \mathbb{C}(x)[s]$ un polynôme de degré au plus 3 divisant $f(s) = sg_2(s)g_3(s)$. $\square$

Proposition 2.4.5 *Nous conservons les notations 2.4.1 et 2.4.2. Nous supposons de plus que B, C et $(1+C)^2 - 4B$ ne sont pas des carrés dans $\mathbb{C}(x)$. Si le point $< g_1, 0 >$ est un double dans $\widetilde{J}(\mathbb{C}(x))$, alors l'une des deux conditions suivantes est vérifiée*

* *$(B-C) \in \mathbb{C}(x)^{\times 2}$, ou*
* *$B(B-C) \in \mathbb{C}(x)^{\times 2}$ et $C(B-C) \in \mathbb{C}(x)^{\times 2}$.*

En particulier, si $B-C$ et BC ne sont pas des carrés dans $\mathbb{C}(x)$, alors $< g_1, 0 >$ n'est pas un double dans $\widetilde{J}(\mathbb{C}(x))$.

Démonstration.

On rappelle que $k_2 = \mathbb{C}(x)[T]/(g_2(T))$ et $k_3 = \mathbb{C}(x)[T]/(g_3(T))$. L'image de $\pi_{\widetilde{\mathcal{C}}}$ est contenue dans le noyau de l'application

$$\begin{array}{ccc} (\mathbb{C}(x)^\times/\mathbb{C}(x)^{\times 2}) \times (k_2^\times/k_2^{\times 2}) \times (k_3^\times/k_3^{\times 2}) & \longrightarrow & \mathbb{C}(x)^\times/\mathbb{C}(x)^{\times 2} \\ (\alpha_1, \alpha_2, \alpha_3) & \longmapsto & \alpha_1 N_{k_2/\mathbb{C}(x)}(\alpha_2) N_{k_3/\mathbb{C}(x)}(\alpha_3) \end{array} .$$

Ainsi, $\pi_{\widetilde{\mathcal{C}},1}(< g_1, 0 >)$ est la classe de $N_{k_2/\mathbb{C}(x)}(-T)N_{k_3/\mathbb{C}(x)}(-T)$ dans $\mathbb{C}(x)^\times/\mathbb{C}(x)^{\times 2}$. Par suite, $< g_1, 0 >$ est un double dans $\widetilde{J}(\mathbb{C}(x))$ si et seulement si les classes

de $-T$ dans k_2 et k_3 sont des carrés.

On commence par donner des conditions nécessaires et suffisantes pour que la classe de $-T$ dans k_2 soit un carré. Soient

$$L_2 := \mathbb{C}(x)[U]/(U^2 - 4C(B-C)^2) \text{ et } \varphi_2 : \begin{array}{ccc} L_2 & \longrightarrow & k_2 \\ U & \longmapsto & T + (1+C)(B-C). \end{array}$$

Le morphisme φ_2 est un isomorphisme. Il induit par passage au quotient un isomorphisme $L_2^\times/L_2^{\times 2} \longrightarrow k_2^\times/k_2^{\times 2}$. L'image de $-U + (1+C)(B-C)$ par ce morphisme étant $-T$, notre problème est de déterminer si $-U + (1+C)(B-C)$ est un carré dans L_2. La norme

$$\begin{array}{rcl} N_{L_2/\mathbb{C}(x)}(-U-(1+C)(B-C)) & = & \mathrm{Res}_U(\ -U+(1+C)(B-C), \\ & & \qquad U^2 - 4C(B-C)^2) \\ & = & (1-C)^2(B-C)^2 \end{array}$$

est bien un carré dans $\mathbb{C}(x)$. La proposition 2.3.2.1 affirme donc que $-U-(1+C)(B-C)$ est un carré dans L_2 si et seulement si $\frac{(1+C)(B-C)+(1-C)(B-C)}{2} = B-C$ ou $\frac{(1+C)(B-C)-(1-C)(B-C)}{2} = C(B-C)$ est un carré dans $\mathbb{C}(x)$. Cela se traduit par : $-T$ est un carré dans k_2 si et seulement si $(B-C)$ ou $C(B-C)$ est un carré dans $\mathbb{C}(x)$.

Il reste à étudier la classe de $-T$ dans k_3. On pose

$$\begin{array}{l} M_3 := \mathbb{C}(x)[V]/(V^2 - (1+C)V + B), \\ L_3 := M_3[U]/(U^2 - V) = \mathbb{C}(x)[U]/(U^4 - (1+C)U^2 + B), \text{ et} \\ \varphi_3 : \begin{array}{ccc} k_3 & \longrightarrow & L_3 \\ T & \longmapsto & d\frac{U+1}{U-1}. \end{array} \end{array}$$

L'isomorphisme φ_3 est correctement défini : B étant différent de C, les polynômes $U-1$ et $U^4-(1+C)U^2+B$ sont premiers entre eux et la classe de $U-1$ dans L_3 est inversible. L'isomorphisme φ_3 induit par passage au quotient un isomorphisme $k_3^\times/k_3^{\times 2} \longrightarrow L_3^\times/L_3^{\times 2}$.

L'image de $-T$ par φ_3 étant $-d\frac{U+1}{U-1}$, nous nous demandons si $d(1-V) = -d(U-1)^2\frac{U+1}{U-1}$ est un carré dans L_3. Comme $d(1-V)$ est un élément de M_3, il ne peut être dans $L_3^{\times 2}$ que si $d(1-V) \in M_3^{\times 2}$ ou $dV(1-V) \in M_3^{\times 2}$. En particulier, lorsque $< g_1, 0 >$ est un double dans $\widetilde{J}(\mathbb{C}(x))$,

$$\begin{array}{rcl} N_{M_3/\mathbb{C}(x)}(d(1-V)) & = & d^2\mathrm{Res}_V(1-V, V^2-(1+C)V+B) \\ & = & d^2(1-(1+C)+B) \\ & = & d^2(B-C) \end{array}$$

$$\begin{array}{rcl} \text{ou } N_{M_3/\mathbb{C}(x)}(dV(1-V)) & = & d^2\mathrm{Res}_V(V(1-V), V^2-(1+C)V+B) \\ & = & d^2B(B-C) \end{array}$$

appartient à $\mathbb{C}(x)^{\times 2}$. $\square$

Notations 2.4.6 *Soit $n \in \mathbb{N}^*$. Nous désignons par $[n]$ la multiplication par n dans $\widetilde{J}(\mathbb{C}(x))$.*

Proposition 2.4.7 *Nous conservons les notations 2.4.1 et 2.4.2.*

Le point $< g_1g_2, 0 >$ est égal à $[2](< (T-d)^2, 16d^2T - 8d^3 >) = [4](< T-d, 8d^3 >)$. En particulier, $< T-d, 8d^3 >$ est un élément de 8-torsion de $\widetilde{J}(\mathbb{C}(x))$.

De plus, le point $< (T-d)^2, 16d^2T - 8d^3 >$ n'est pas τ-invariant.

Démonstration.

Nous appliquons le théorème 2.3.1.2 avec $u = g_1g_2$, $w = -g_3$ et $v = 0$. Pour cela, nous considérons l'égalité

$$(U^2-1)(U^2-C) - (U^4 - (1+C)U + B) = C - B$$

et nous effectuons le changement de variable $U = \frac{s+d}{s-d}$. On obtient ainsi l'égalité

$$4d(1-C)g_1(s)g_2(s) - (B-C)g_3 = -(B-C)(s-d)^4.$$

On pose $u_1 := (s-d)^2$, $q := 2(1-C)$ et r le reste de la division euclidienne de $v_1 := qg_1g_2$ par u_1. Nous venons de montrer que le couple (u, q) est solution de l'équation :

$$-u_1^2 = -g_3 + q^2 g_1 g_2,$$

c'est-à-dire de l'équation

$$(-1)^{\deg(u)} u_1^2 = a^2 w + 2qav + q^2 u$$

avec $a := 1$. Nous pouvons donc appliquer le théorème 2.3.1.2 : $< g_1g_2, 0 >= [2] < u, r >$.

Le reste de la division euclidienne de $g_2(s) = s^2 + 2(1+C)(B-C)s + d^2$ par $(s-d)^2$ est $2(1+C)(B-C)s + 2ds = 4(B-C)s$, donc

$$\begin{aligned} v_1 = 2(1-C)sg_2 &\equiv 8ds^2 \bmod (s-d)^2 \\ &\equiv 16d^2 s - 8d^3 \bmod (s-d)^2. \end{aligned}$$

On en déduit que $r = 16d^2s - 8d^3$.

Il nous reste à vérifier que $< u_1, r >$ n'est pas τ-invariant. Nous calculons la réduction de

$$-\frac{s^4}{d^4}\tau(r) = -8\frac{s^4}{d^2}\left(\frac{2d^2}{s} - d\right) = 8\frac{s^4}{d} - 16s^3$$

modulo $(s-d)^2$ à l'aide des congruences

$$\begin{aligned} s^3 &= ((s-d)+d)^3 \equiv 3d^2(s-d) + d^3 \bmod (s-d)^2 \text{ et} \\ s^4 &= ((s-d)+d)^4 \equiv 4d^3(s-d) + d^4 \bmod (s-d)^2. \end{aligned}$$

On obtient :

$$\begin{aligned} -\tfrac{s^4}{d^4}\tau(r) &\equiv 8(4d^2(s-d)+d^3) - 16(3d^2(s-d)+d^3) \bmod (s-d)^2 \\ &\equiv -16d^2(s-d) - 8d^3 \bmod (s-d)^2 \\ &\equiv -r \bmod (s-d)^2. \end{aligned}$$

Le théorème 2.2.4 nous assure donc que le point $< (s-d)^2, r >$ n'est pas τ-invariant. $\square$

Corollaire 2.4.8 *Soient B et C deux éléments de $\mathbb{R}(x)$. Soit $\mathcal{C}$ la courbe hyperelliptique d'équation affine*

$$z^2 + (y^2+1)(y^2+C)(y^4+(1+C)y^2+B) = 0.$$

Soit J la jacobienne de la courbe $\mathcal{C}$. On suppose que B, C, BC, $B-C$, $(B-C)(1-C)$ et $(1+C)^2-4B$ ne sont pas des carrés dans $\mathbb{C}(x)$.

Alors la torsion 2-primaire de $J(\mathbb{C}(x))$ est de cardinal fini.

Démonstration.

Comme C est non nul, le polynôme y^2+C est sans facteur carré. De plus, $1-C$ est non nul donc y^2+1 et y^2+C sont premiers entre eux. De même $B-C$ est non nul donc $(y^2+1)(y^2+C)$ et $y^4+(1+C)y^2+B$ sont premiers entre eux. Or le discriminant $16B((1-C)^2-4B)^2$ de $y^4+(1+C)y^2+B$ est non nul, donc le polynôme $(y^2+1)(y^2+C)(y^4+(1+C)y^2+B)$ est sans facteur carré.

Nous reprenons les notations 2.4.2 : nous posons $d := (1-C)(B-C)$,

$$\begin{aligned} g_1(s) &:= s, \\ g_2(s) &:= \tfrac{-(s+d)^2+C(s-d)^2}{C-1} \text{ et} \\ g_3(s) &:= \tfrac{(s+d)^4-(1+C)(s+d)^2(s-d)^2+B(s-d)^4}{B-C} \end{aligned}$$

La courbe $\mathcal{C}$ est birationnellement équivalente à la courbe hyperelliptique $\widetilde{\mathcal{C}}$ d'équation affine

$$\widetilde{\mathcal{C}} : t^2 = f(s) \text{ avec } f(s) = g_1(s)g_2(s)g_3(s).$$

Soit $\widetilde{J}$ la jacobienne de la courbe $\widetilde{\mathcal{C}}$.

D'après la proposition 2.4.4, la 2-torsion $\mathbb{C}(x)$-rationnelle de $\widetilde{J}$ est engendrée par $< g_1, 0 >$ et $< g_2, 0 >$, c'est-à-dire par $< g_2, 0 >$ et $< g_1g_2, 0 >= [4] < T-d, 8d^3 >$.

Soit T un point de 4 -torsion. Alors $2T$ est un point de 2-torsion : il existe n_1, $n_2 \in \{0,1\}$ tels que $[2]T = [n_1] < g_2, 0 > +[4n_2] < T-d, 8d^3 >$. Or, d'après la proposition 2.4.5, le point $< g_2, 0 >$ n'appartient pas à $2\widetilde{J}(\mathbb{C}(x))$, donc $n_1 = 0$. Ainsi, le groupe des points $\mathbb{C}(x)$-rationnels de 4-torsion est engendré par $< g_2, 0 >$ et $[2] < T-d, 8d^3 >$.

Nous montrons de même que le groupe des points $\mathbb{C}(x)$-rationnels de 8-torsion est engendré par $< g_2, 0 >$ et $< T-d, 8d^3 >$.

Soit $\pi_{\widetilde{\mathcal{C}}}$ le morphisme de Cassels-Schaefer associé à $\widetilde{J}(\mathbb{C}(x))$. Un point $< u, v >$ appartient à $2\widetilde{J}(\mathbb{C}(x))$ si et seulement si son image par $\pi_{\widetilde{\mathcal{C}}}$ est triviale. En particulier, si $< u, v > \in 2\widetilde{J}(\mathbb{C}(x))$ et si u est premier à f, alors $(-1)^{\deg(u)}u(0)$ est un carré dans $\mathbb{C}(x)$.

Supposons qu'il existe un élément de 16-torsion de $\widetilde{J}(\mathbb{C}(x))$ qui ne soit pas de 8-torsion. Le double de T est alors de la forme $< T-d, 8d^3 > + n < g_2, 0 >$ avec $n \in \{0, 1\}$. Or $\pi_{\widetilde{\mathcal{C}}}$ est un morphisme de groupe et $(-1)^{\deg(g_2)}g_2(0) = d^2$, donc $d = (-1)^{\deg_T(T-d)}(0-d)$ est un carré dans $\mathbb{C}(x)$. Ceci est en contradiction avec les hypothèses. Les éléments de 16-torsion de $\widetilde{J}(\mathbb{C}(x))$ sont donc tous de 8-torsion. Par suite, la torsion 2-primaire $J(\mathbb{C}(x))$ est de cardinal fini. $\square$

Théorème 2.4.9 *Soient B et C deux éléments distincts de $\mathbb{R}(x)$. On suppose que B, C, BC, $B-C$ et $(1+C)^2-4B$ ne sont pas des carrés dans $\mathbb{C}(x)$. Soit $\mathcal{C}$ la courbe hyperelliptique d'équation affine*

$$\mathcal{C} : z^2 + (y^2+1)(y^2+C)(y^4+(1+C)y^2+B) = 0.$$

Alors $Jac(\mathcal{C})(\mathbb{R}(x))$ ne contient aucun point de torsion antineutre.

Démonstration.

Comme C est non nul, le polynôme y^2+C est sans facteur carré. De plus, $1-C$ est non nul donc y^2+1 et y^2+C sont premiers entre eux. De même $B-C$ est non nul donc $(y^2+1)(y^2+C)$ et $y^4+(1+C)y^2+B$ sont premiers entre eux. Or le discriminant $16B((1-C)^2-4B)^2$ de $y^4+(1+C)y^2+B$ est non nul, donc le polynôme $(y^2+1)(y^2+C)(y^4+(1+C)y^2+B)$ est sans facteur carré.

Nous reprenons les notations 2.4.2 : nous posons $d := (1-C)(B-C)$,

$$\begin{array}{lcl} g_1(s) & := & s, \\ g_2(s) & := & \frac{-(s+d)^2+C(s-d)^2}{C-1} \text{ et} \\ g_3(s) & := & \frac{(s+d)^4-(1+C)(s+d)^2(s-d)^2+B(s-d)^4}{B-C} \end{array}$$

La courbe $\mathcal{C}$ est birationnellement équivalente à la courbe hyperelliptique $\widetilde{\mathcal{C}}$ d'équation affine

$$\widetilde{\mathcal{C}} : t^2 = f(s) \text{ avec } f(s) = g_1(s)g_2(s)g_3(s).$$

Soit $\widetilde{J}$ la jacobienne de la courbe $\widetilde{\mathcal{C}}$. Soient σ la conjugaison complexe et

$$\begin{array}{rccc} \tau : & \mathbb{C}(x)(\widetilde{\mathcal{C}}) & \longrightarrow & \mathbb{C}(x)(\widetilde{\mathcal{C}}) \\ & a(s)t+b(s) & \longmapsto & -\sigma(a)\left(\frac{d^2}{s}\right)\frac{d^4t}{s^4} + \sigma(b)\left(\frac{d^2}{s}\right). \end{array}$$

D'après la proposition 2.4.4, la 2-torsion $\mathbb{C}(x)$-rationnelle de $\widetilde{J}$ est engendrée par $< g_1, 0 >$ et $< g_2, 0 >$. Puisque $s^2\tau(s) = d^2 s$ et

$$\begin{aligned} s^2\tau(g_2(s)) &= \tfrac{s^2}{C-1}\tau(-(s+d)^2 + C(s-d)^2) \\ &= d^2\tfrac{-(s+d)^2+C(s-d)^2}{C-1} = d^2 g_2(s), \end{aligned}$$

les points $< s, 0 >$ et $< g_2, 0 >$ sont τ-invariants (voir le théorème 2.2.4). De plus, les diviseurs $< g_1, 0 >$ et $< g_2, 0 >$ sont de poids strictement inférieurs à 3. D'après le théorème 2.2.4, pour tout point $\beta \in \widetilde{J}(\mathbb{C}(x))$ et tout point de 2-torsion $\alpha \in \widetilde{J}(\mathbb{C}(x))$, on a équivalence entre :

* β est τ-antineutre
* $\beta + \alpha$ est τ-antineutre.

D'après la proposition 2.4.5 le point $< g_1, 0 >$ n'est pas un double dans $\widetilde{J}(\mathbb{C}(x))$. Ainsi la proposition 2.4.7 décrit la 4-torsion de $\widetilde{J}(\mathbb{C}(x))$: elle est engendrée par $< g_1, 0 >$ et $< (T-d)^2, 16d^2T - 8d^3 >$. Le point $< (T-d)^2, 16d^2T - 8d^3 >$ n'est pas τ-invariant (c.f. la proposition 2.4.7) et donc pas τ-antineutre. Par suite $\widetilde{J}(\mathbb{C}(x))$ n'a aucun élément de torsion 2-primaire τ-antineutre. Pour conclure nous utilisons le corollaire 2.1.3 : $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ ne contient aucun élément de torsion 2-primaire antineutre. □

2.5 Des exemples de polynômes de la forme $(y^2+1)(y^2+a(x))(y^2+b(x))(y^2+c(x))$ qui sont sommes de trois carrés dans $\mathbb{R}(x,y)$

Au cours de cette section nous souhaitons écrire sous la forme d'une somme de trois carrés dans $\mathbb{R}(x,y)$ un polynôme

$$P(x,y) = (y^2+1)(y^2+a(x))(y^2+b(x))(y^2+c(x)),$$

où $a(x)$, $b(x)$, et $c(x) \in \mathbb{R}(x)$ désignent trois fractions rationnelles totalement positives. Ceci n'est pas toujours possible et nous souhaitons mettre en évidence des conditions suffisantes sur les coefficients a, b et c pour que le polynôme $P(x,y)$ soit somme de trois carrés dans $\mathbb{R}(x,y)$.

Notations 2.5.0.2 Soient a, b et c trois éléments de $\mathbb{R}(x)$ totalement positifs. Nous supposons le polynôme $P(x,y) = (y^2+1)(y^2+a)(y^2+b)(y^2+c)$ sans facteur carré c'est-à-dire que les fractions rationnelles 1, a, b et c sont non nulles et deux à deux distinctes.

Soit $\mathcal{C}$ la $\mathbb{R}(x)$-courbe hyperelliptique d'équation affine

$$\mathcal{C} : z^2 + (y^2+1)(y^2+a)(y^2+b)(y^2+c) = 0.$$

Soit J la jacobienne de la courbe $\mathcal{C}$.

Notre problème est de trouver des points de $J(\mathbb{R}(x))$ qui soient antineutres. La stratégie choisie est la recherche de points de torsion 2-primaire antineutres. Pour calculer les éléments de torsion 2-primaire de $J(\mathbb{R}(x))$, nous avons besoin d'un moyen de manipuler les éléments de $J(\mathbb{C}(x))$. Ceci a déjà été discuté à la section 2.1.

Notations 2.5.0.3 Nous posons $d = (1-a)(1-b)(1-c)$. À tout élément $\alpha \in \mathbb{C}(x)$ nous associons le polynôme

$$g_\alpha(s) := s^2 + 2d\frac{1+\alpha}{1-\alpha}s + d^2.$$

Soit $\begin{array}{rccc} \Gamma : & \mathbb{C}(x)(\mathcal{C}) & \longrightarrow & \mathbb{C}(x)(\widetilde{\mathcal{C}}) \\ & A(y,z) & \longmapsto & A\left(i\frac{s+d}{s-d}, \frac{2idt}{(s-d)^4}\right) \end{array}$. D'après le théorème 2.1.1, l'isomorphisme Γ induit une équivalence birationnelle sur $\mathbb{C}(x)$ entre la courbe $\mathcal{C}$ et la courbe $\widetilde{\mathcal{C}}$ d'équation affine

$$\widetilde{\mathcal{C}} : t^2 = s g_a(s) g_b(s) g_c(s).$$

On note $\widetilde{J}$ la jacobienne de la courbe $\widetilde{\mathcal{C}}$.

Pour $\alpha \in \mathbb{C}(x)$, on note $k_\alpha := \mathbb{C}(x)[T]/(g_\alpha(T))$. Soient

$$\pi_{\widetilde{\mathcal{C}}} : \widetilde{J}(\mathbb{C}(x)) \longrightarrow \mathbb{C}(x)^\times/\mathbb{C}(x)^{\times 2} \times k_a^\times/k_a^{\times 2} \times k_b^\times/k_b^{\times 2} \times k_c^\times/k_c^{\times 2}$$

le morphisme de Cassels-Schaefer associé à $\widetilde{J}(\mathbb{C}(x))$ et $\pi_{\widetilde{\mathcal{C}},\alpha} : \widetilde{J}(\mathbb{C}(x)) \longrightarrow k_\alpha^\times/k_\alpha^{\times 2}$ la coordonnée de $\pi_{\widetilde{\mathcal{C}}}$ associée à g_α. Si $\mathrm{div}(u,v) \in \mathrm{Div}^0(\mathbb{C}(x)(\widetilde{\mathcal{C}})$ est un représentant d'une classe d'équivalence linéaire $D \in \widetilde{J}(\mathbb{C}(x))$ tel que u soit premier à g_α, alors $\pi_{\widetilde{\mathcal{C}},\alpha}(D)$ est la classe de $(-1)^{\deg(u)}u(T)$ dans $k_\alpha^\times/k_\alpha^{\times 2}$.

On définit enfin à l'aide de la conjugaison complexe σ une involution

$$\begin{array}{rccc} \tau : & \mathbb{C}(x)(\widetilde{\mathcal{C}}) & \longrightarrow & \mathbb{C}(x)(\widetilde{\mathcal{C}}) \\ & a(s)t + b(s) & \longmapsto & -\sigma(a)\left(\frac{d^2}{s}\right)\frac{d^4 t}{s^4} + \sigma(b)\left(\frac{d^2}{s}\right). \end{array}$$

Nous faisons appel au corollaire 2.1.3 : notre objectif est maintenant de trouver des conditions sur a, b et c sous lesquelles $\widetilde{J}(\mathbb{C}(x))$ a un élément τ-antineutre. Le calcul de la 2^n-torsion est effectué en suivant la méthode énoncée lors de la sous-section 2.3.2. Nous distinguons des cas suivant la forme des paramètres a, b et c.

2.5.1 Existence de points de 2-torsion antineutres.

Le polynôme $f(s) = d^6(s-d)^8 Q(x, -\left(\frac{s+d}{s-d}\right)^2)$ est sans facteur carré puisque Q a lui même été supposé sans facteur carré et de degré 8. Nous pouvons donc utiliser la représentation de Mumford pour manipuler les éléments de $\widetilde{J}$.

La 2-torsion $\mathbb{C}(x)$-rationnelle de la jacobienne de la courbe $\widetilde{\mathcal{C}}$ est connue : elle est engendrée par les diviseurs de représentation de Mumford $(u, 0)$ où u désigne un diviseur de poids au plus 3 du polynôme $f(s)$.

Lemme 2.5.1.1 *Soit k un corps de caractéristique différente de 2. Soit d, $\alpha \in k$. On suppose $\alpha \neq 1$.*

Alors, le polynôme $T^2+2d\frac{1+\alpha}{1-\alpha}T+d^2$ est irréductible sur k si et seulement si α n'est pas un carré dans k.

De plus, s'il existe $\beta \in k$ tel que $\alpha = \beta^2$, alors $T^2 + 2d\frac{1+\alpha}{1-\alpha}T + d^2$ se factorise sous la forme $T^2 + 2d\frac{1+\alpha}{1-\alpha}s + d^2 = (T + d\frac{1+\beta}{1-\beta})(T + d\frac{1-\beta}{1+\beta})$.

Démonstration.

Nous notons $\bar{k}$ une clôture algébrique de k. Dans le corps $\bar{k}$, le polynôme $T^2 + 2d\frac{1+\alpha}{1-\alpha}T + d^2$ s'écrit alors sous la forme

$$T^2 + 2d\frac{1+\alpha}{1-\alpha}T + d^2 = \left(T + d\frac{1+\alpha}{1-\alpha}\right)^2 - \left(\frac{4d^2\alpha}{(1-\alpha)^2}\right).$$

Ses deux racines dans $\bar{k}$ sont dans k si et seulement si α est un carré dans k. De plus, si $\beta \in \bar{k}$ est de carré égal à α, alors les racines de $T^2+2d\frac{1+\alpha}{1-\alpha}T+d^2$ sont égales à $d\frac{1+\beta^2}{1-\beta^2} + \frac{2d\beta}{1-\beta^2} = d\frac{(1+\beta)^2}{1-\beta^2} = d\frac{1+\beta}{1-\beta}$ et $d\frac{1+\beta^2}{1-\beta^2} - \frac{2d\beta}{1-\beta^2} = d\frac{1-\beta}{1+\beta}$. □

Proposition 2.5.1.2 *On conserve les notations 2.5.0.2 et 2.5.0.3. La 2-torsion de la jacobienne $\widetilde{J}(\mathbb{C}(x))$ est engendrée par les points*

* $< s, 0 >$,
* $< g_a(s), 0 >$ *et, si* $a = \alpha^2$ *pour un certain* $\alpha \in \mathbb{C}(x)$, *par* $< s + d\frac{1+\alpha}{1-\alpha}, 0 >$ *et* $< s + d\frac{1-\alpha}{1+\alpha}, 0 >$,
* $< g_b(s), 0 >$ *et, si* $b = \beta^2$ *pour un certain* $\beta \in \mathbb{C}(x)$, *par* $< s + d\frac{1+\beta}{1-\beta}, 0 >$ *et* $< s + d\frac{1-\beta}{1+\beta}, 0 >$, *et*
* $< g_c(s), 0 >$ *et, si* $c = \gamma^2$ *pour un certain* $\gamma \in \mathbb{C}(x)$, *par* $< s + d\frac{1+\gamma}{1-\gamma}, 0 >$ *et* $< s + d\frac{1-\gamma}{1+\gamma}, 0 >$.

Étant de poids 2, le point $< g_a, 0 >$ ne peut être τ-antineutre. En fait, d'après le théorème 2.2.4, pour tout élément $D \in \widetilde{J}$, on a équivalence entre la τ-antineutralité de D et celle de $D+ < g_a, 0 >$. Par symétrie du rôle de a, b et c, cette remarque s'applique aussi à $< g_b, 0 >$ et $< g_c, 0 >$.

De même, la τ-antineutralité de tout $D \in \widetilde{J}$ est équivalente à celle de $D+ < s, 0 >$. Nous ne pouvons donc espérer obtenir un point de 2-torsion τ-antineutre qu'en sommant des diviseurs du type $< s + d\frac{1+\alpha}{1-\alpha}, 0 >$, lorsque c'est possible. Un point τ-antineutre devant être de poids 3, la seule possibilité est le diviseur $< (s + d\frac{1+\alpha}{1-\alpha})(s + d\frac{1+\beta}{1-\beta})(s + d\frac{1+\gamma}{1-\gamma}), 0 >$ dans le cas où $a = \alpha^2$, $b = \beta^2$ et $c = \gamma^2$ (les fractions rationnelles α, β et γ sont à coefficients réels puisque les fractions rationnelles a, b $c \in \mathbb{R}(x)$ sont totalement positives).

Proposition 2.5.1.3 *On conserve les notations 2.5.0.2 et 2.5.0.3. On suppose qu'il existe* α, β *et* $\gamma \in \mathbb{R}(x)$ *tels que* $a = \alpha^2$, $b = \beta^2$ *et* $c = \gamma^2$.

Alors la classe d'équivalence linéaire du diviseur

$$D := < (s + d\frac{1+\alpha}{1-\alpha})(s + d\frac{1+\beta}{1-\beta})(s + d\frac{1+\gamma}{1-\gamma}), 0 >$$

est un élément de 2-torsion τ*-antineutre de* $Jac(\widetilde{\mathcal{C}})(\mathbb{C}(x))$.

Par suite le polynôme $P(y) = (y^2+1)(y^2+a)(y^2+b)(y^2+c)$ *est une somme de trois carrés (en fait deux carrés) dans* $\mathbb{R}(x, y)$ *:*

$$\begin{aligned} P(y) &= ((\alpha+\beta+\gamma-1)y^3 + (\alpha\beta+\alpha\gamma+\beta\gamma-\alpha\beta\gamma)y)^2 \\ &\quad +(-y^4 + (\alpha\beta+\alpha\gamma+\beta\gamma-\alpha-\beta-\gamma)y^2 + \alpha\beta\gamma)^2. \end{aligned}$$

Remarque :

Le produit de deux sommes de deux carrés est une somme de deux carrés. La proposition 2.5.1.3 illustre la possibilité de retrouver certaines formules classiques concernant les produits de sommes de carrés en considérant des points de torsions antineutres. La démonstration de la proposition 2.5.1.3 n'est pas reproduite ici. Elle est est analogue à la démonstration du théorème 2.5.2.8.

2.5.2 Des conditions d'existence de $\mathbb{C}(x)$-points de 4-torsion

Nous étudions une partie de la 4-torsion de $J(\mathbb{R}(x))$. Plus précisément nous cherchons un élément de 4-torsion antineutre de $J(\mathbb{R}(x))$. Nous en déduisons une formule de multiplicativité de certaine sommes de trois carrés.

Nous commençons par étudier les conditions sous lesquelles certains points de 2-torsion sont des doubles dans $\widetilde{J}(\mathbb{C}(x))$ en calculant leurs images par le morphisme de Cassels-Schaefer $\pi_{\widetilde{\mathcal{C}}}$. associé à la courbe $\widetilde{\mathcal{C}}$.

Notations 2.5.2.1 *Afin de simplifier les énoncés, nous posons* $S_- := s - d$.

À une fraction rationnelle $\alpha \in \mathbb{C}(x)$, *nous avons associé le polynôme* $g_\alpha(s) := s^2 + 2d\frac{1+\alpha}{1-\alpha}s + d^2$. *À cette fraction rationnelle* α *nous faisons également correspondre la* $\mathbb{C}(x)$*-algèbre* $K_{T^2-g_\alpha} := \mathbb{C}(x, s)[T]/(T^2 - g_\alpha)$.

Le lemme suivant permet de déterminer si l'image par $\pi_{\widetilde{\mathcal{C}}}$ d'un point de 2-torsion fixé est triviale.

Lemme 2.5.2.2 *Soit* k *un corps de caractéristique différente de* 2.

Soit d, λ, $\alpha \in k$. *On suppose que* α *n'est égal ni à* 1 *ni à* -1, *et que* d *et* λ *sont non nuls.*
On note $g_\alpha(T) := T^2 + 2d\frac{1+\alpha}{1-\alpha}T + d^2$ *et* $k_\alpha := k[U]/(g_\alpha(U))$.
On a alors équivalence entre :

* $d\lambda(1-\alpha)U \in k_\alpha^{\times 2}$ *et*
* $-\lambda \in k^{\times 2}$ *ou* $-\alpha\lambda \in k^{\times 2}$.

De plus, pour tout $\lambda_2 \in k$, les deux égalités suivantes sont vérifiées :

$$\left(\frac{\lambda_2(1-\alpha)}{2}(U-d)\right)^2 = -d(1-\alpha)\lambda_2^2 U \text{ et}$$
$$\left(\frac{\lambda_2(1-\alpha)}{2}(U+d)\right)^2 = -d(1-\alpha)\alpha\lambda_2^2 U$$

Démonstration.

Nous utilisons l'égalité $g_\alpha = T^2 + 2d\frac{1+\alpha}{1-\alpha}T + d^2 = (T-d)^2 + \frac{4d}{1-\alpha}T$. Elle signifie que $d\lambda(1-\alpha)U = -\lambda\left(\frac{(1-\alpha)(T-d)}{2}\right)^2$. Par suite, $d\lambda(1-\alpha)U$ appartient à $k_\alpha^{\times 2}$ si et seulement si $-\lambda \in k_\alpha^{\times 2}$.

Soient $L := k[V]/(V^2-\alpha)$ et $\varphi : L \longrightarrow k_\alpha$ l'unique k-isomorphisme tel que $\varphi(V) = \frac{1-\alpha}{2d}\left(U + \frac{1+\alpha}{1-\alpha}\right)$. L'isomorphisme φ induit par passage au quotient un isomorphisme de $L^\times/L^{\times 2}$ dans $k_\alpha^\times/k_\alpha^{\times 2}$. Ainsi $-\lambda$ est un carré dans k_α si et seulement si $-\lambda$ est un carré dans L.

L'extension L/k satisfait les conditions d'application de la proposition 2.3.2.1. Par suite, $-\lambda$ est un carré dans L si et seulement si $-\lambda \in k^{\times 2}$ ou $-\lambda\alpha \in k^{\times 2}$. □

Remarque :

Heuristiquement, on trouve les deux formules énoncées dans le lemme 2.5.2.2 grâce à la proposition 2.3.2.1 : cette proposition nous donne un moyen d'écrire $\varphi^{-1}(d(1-\alpha)\lambda U)$ comme un carré dans L à chaque fois que c'est possible.

Corollaire 2.5.2.3 *Soit k un corps de caractéristique différente de 2.*

Soit d, λ, α, $\beta \in k$. On suppose que α n'est égal ni à 1 ni à -1, que β est différent de 1, et que d et λ sont non nuls.

Pour tout $\gamma \in k$, on note $g_\gamma(T) := T^2 + 2d\frac{1+\gamma}{1-\gamma}T + d^2$ et $k_\gamma := k[U]/(g_\gamma(U))$.

Alors $g_\beta(U)$ est un carré dans k_α si et seulement si $(\alpha-\beta)(1-\beta) \in k^{\times 2}$ ou $\alpha(\alpha-\beta)(1-\beta) \in k^{\times 2}$. On a de plus :

$$(1-\beta)g_\beta(T) = (\alpha-\beta)(T-d)^2 + (1-\alpha)g_\alpha \text{ et}$$
$$\alpha(1-\beta)g_\beta = (\alpha-\beta)(T+d)^2 + \beta(1-\alpha)g_\alpha.$$

Démonstration.

On applique le lemme 2.5.2.2 en utilisant l'égalité $g_\beta(T) - g_\alpha(T) = 4d\frac{\beta-\alpha}{(1-\alpha)(1-\beta)}T$ (en particulier $g_\beta(U) = 4d\frac{\beta-\alpha}{(1-\alpha)(1-\beta)}U$). □

Corollaire 2.5.2.4 *Soit k un corps de caractéristique différente de 2.*

Soit d, λ, α, β, $\gamma \in k$. On suppose que α n'est égal ni à 1 ni à -1, que β et γ sont différents de 1, et que d et λ sont non nuls.

Pour tout $\eta \in k$, on note $g_\eta(T) := T^2 + 2d\frac{1+\eta}{1-\eta}T + d^2$. Soit $k_\alpha := k[U]/(g_\alpha(U))$.

Alors $-Ug_\beta(U)g_\gamma(U)$ est un carré dans k_α si et seulement si

* $d(\beta-\alpha)(\gamma-\alpha)(1-\alpha)(1-\beta)(1-\gamma) \in k^{\times 2}$ *ou*
* $d\alpha(\beta-\alpha)(\gamma-\alpha)(1-\alpha)(1-\beta)(1-\gamma) \in k^{\times 2}$.

Démonstration.

Pour tout $\eta \in k$, on a l'égalité $g_\eta(T) - g_\alpha(T) = 4d\frac{\eta-\alpha}{(1-\eta)(1-\eta)}T$. Ainsi, $-Ug_\beta(U)g_\gamma(U) = -16d^2\frac{(\beta-\alpha)(\gamma-\alpha)}{(1-\alpha)^2(1-\beta)(1-\gamma)}U^3$ et le corollaire 2.5.2.4 est une conséquence du lemme 2.5.2.2 $\square$

Proposition 2.5.2.5 *On conserve les notations 2.5.0.2, 2.5.0.3 et 2.5.2.1. Le point $< s, 0 >$ a un antécédent $\mathbb{C}(x)$-rationnel par la multiplication par 2 si et seulement si les trois conditions suivantes sont vérifiées :*

1. $(1-b)(1-c) \in \mathbb{C}(x)^{\times 2}$ *ou* $a(1-b)(1-c) \in \mathbb{C}(x)^{\times 2}$,
2. $(1-a)(1-c) \in \mathbb{C}(x)^{\times 2}$ *ou* $b(1-a)(1-c) \in \mathbb{C}(x)^{\times 2}$, *et*
3. $(1-a)(1-b) \in \mathbb{C}(x)^{\times 2}$ *ou* $c(1-a)(1-b) \in \mathbb{C}(x)^{\times 2}$.

Remarque :

La proposition 2.5.2.5 se démontre en cherchant les conditions sous lesquelles l'image $\pi_{\widetilde{\mathcal{C}}}(< s, 0 >)$ est triviale, c'est-à-dire les conditions sous lesquelles s est un carré modulo g_a, g_b et g_c. Ces conditions nous sont données par le lemme 2.5.2.2.

Remarque :

Nous nous plaçons sous les hypothèses de la proposition 2.5.2.5. Si $(1-b)(1-c) = \alpha^2$ et $(1-a)(1-c) = \beta^2$ avec α, $\beta \in \mathbb{C}(x)$, alors le point $< s, 0 >$ a un antécédent pour la multiplication par 2 qui est τ-antineutre si et seulement si $a - 1 = \gamma^2$ avec $\gamma \in k$. Dans ce cas les éléments

$$\begin{aligned} y^2 + a &= y^2 + 1 + \gamma^2, \\ y^2 + b &= y^2 + 1 + \left(\frac{\alpha\gamma}{\beta}\right)^2 \text{ et} \\ y^2 + c &= y^2 + 1 + \left(\frac{\alpha}{\gamma}\right)^2 \end{aligned}$$

sont dans l'image de $N_{K_{T^2+y^2+1}/\mathbb{R}(x,y)}$. Par multiplicativité de $N_{K_{T^2+y^2+1}/\mathbb{R}(x,y)}$, le produit $P(x,y) = (y^2+1)(y^2+a)(y^2+B)(y^2+c)$ est aussi dans l'image de $N_{K_{T^2+y^2+1}/\mathbb{R}(x,y)}$: le polynôme $P(x,y)$ est alors écrit sous la forme d'une somme de trois carrés dans $\mathbb{R}(x,y)$.

En fait, à chaque fois qu'il existe un point de 4-torsion antineutre de $\widetilde{J}(\mathbb{C}(x))$ de double $< s, 0 >$, il est possible d'écrire $P(y)$ comme somme de trois carrés dans $\mathbb{R}(x,y)$ en utilisant la multiplicativité de la norme $N_{K_{T^2+y^2+1}/\mathbb{R}(x,y)}$ relative à l'extension $K_{T^2+y^2+1} := \mathbb{R}(x,y)[T]/(T^2+y^2+1)$ de $\mathbb{R}(x,y)$.

La proposition 2.5.2.5 n'est donc donnée qu'à titre d'indication.

Proposition 2.5.2.6 *On conserve les notations 2.5.0.2, 2.5.0.3 et 2.5.2.1. Le point* $< g_a(s), 0 >$ *appartient à* $2\widetilde{J}(\mathbb{C}(x))$ *si et seulement si les trois conditions suivantes sont vérifiées :*

1. $(b-a)(c-a) \in \mathbb{C}(x)^{\times 2}$ *ou* $a(b-a)(c-a) \in \mathbb{C}(x)^{\times 2}$,
2. $(b-a)(1-a) \in \mathbb{C}(x)^{\times 2}$ *ou* $b(b-a)(1-a) \in \mathbb{C}(x)^{\times 2}$, *et*
3. $(c-a)(1-a) \in \mathbb{C}(x)^{\times 2}$ *ou* $c(c-a)(1-a) \in \mathbb{C}(x)^{\times 2}$.

Démonstration.

Le point $< g_a(s), 0 >$ appartient à $2\widetilde{J}(\mathbb{C}(x))$ si et seulement si l'image $\pi_{\widetilde{\mathcal{C}}}(< g_a(s), 0 >)$ est triviale. Nous calculons $\pi_{\widetilde{\mathcal{C}}}(< g_a(s), 0 >)$ en remarquant que $< g_a, 0 > + < sg_bg_c, 0 >= 0$: le morphisme $\pi_{\widetilde{\mathcal{C}}}$ est à valeur dans un groupe d'exposant 2, donc $\pi_{\widetilde{\mathcal{C}}}(< g_a, 0 >) = \pi_{\widetilde{\mathcal{C}}}(< sg_bg_c, 0 >)$.

Puisque $g_a(T)$ est premier à $g_b(T)g_c(T)$ (nous rappelons que nous avons supposé f sans facteur carré) et de degré 2, l'image $\pi_{\widetilde{\mathcal{C}},\alpha}(< g_a, 0 >)$ est la classe de $g_a(T)$ dans $k_\alpha^\times / k_\alpha^{\times 2}$ (pour $\alpha = b$ ou c). La relation de primalité relative de $g_a(T)$ et $Tg_b(T)g_c(T)$ nous permet également d'affirmer que l'image $\pi_{\widetilde{\mathcal{C}},a}(< g_a, 0 >) = \pi_{\widetilde{\mathcal{C}},a}(< sg_bg_c, 0 >)$ est la classe de $-Tg_a(T)g_b(T)$ dans $k_a^\times / k_a^{\times 2}$.

Nous faisons maintenant appel à la proposition 1.5.9 : les coordonnées $\pi_{\widetilde{\mathcal{C}},a}$ $\pi_{\widetilde{\mathcal{C}},b}$ et $\pi_{\widetilde{\mathcal{C}},c}$ suffisent à déterminer si $< g_a(s), 0 >$ est un élément de $2\widetilde{J}(\mathbb{C}(x))$. Ainsi, $< g_a, 0 > \in 2\widetilde{J}(\mathbb{C}(x))$ si et seulement si $-Tg_bg_c \in k_a^{\times 2}$, $g_a \in k_b^{\times 2}$ et $g_a \in k_c^{\times 2}$. Nous pouvons dès lors conclure en faisant appel aux corollaires 2.5.2.3 et 2.5.2.4.

Proposition 2.5.2.7 *On conserve les notations 2.5.0.2, 2.5.0.3 et 2.5.2.1. On suppose l'existence de deux fractions rationnelles* β, $\gamma \in \mathbb{C}(x)$ *telles que* $(b-a) = \beta^2(1-a)$ *et* $(c-a) = \gamma^2(1-a)$.

Alors $< g_a, 0 >$ *est égal à* $2 < u, v >$ *avec :*

* $u := \frac{(\beta\gamma S_-^2 + (1+\beta+\gamma)g_a)S_-}{(1+\beta)(1+\gamma)}$,
* $q := \frac{(1-a)^2(g_a + (\beta\gamma+\beta+\gamma)S_-^2)}{2d}$ *et*
* v *le reste de la division euclidienne de* qg_a *par* u.

De plus, si β, $\gamma \in i\mathbb{R}(x)$, *alors* $< u, v >$ *est* τ*-invariant et*

$$\tau(div(u,v)) - div(u,v) = div\left(\frac{2dt + (1-a)^2(g_a - S_-^2)(g_a + \beta\gamma S_-^2)}{2dsu(s)}\right).$$

Démonstration.

D'après le lemme 2.5.2.2 et le corollaire 2.5.2.3, nous pouvons affirmer que $-\frac{4d}{1-a}s = N_{K_{T^2-g_a}/\mathbb{C}(x,s)}(T + S_-)$, $-\frac{1-b}{1-a}g_b = N_{K_{T^2-g_a}/\mathbb{C}(x,s)}(T + \beta S_-)$

et $-\frac{1-c}{1-a}g_c = N_{K_{T^2-g_a}/\mathbb{C}(x,s)}(T+\gamma S_-)$. Nous déduisons de ces trois égalités et de la multiplicativité de $N_{K_{T^2-g_a}/\mathbb{C}(x,s)}$ que

$$\begin{aligned} -\tfrac{4d^2}{(1-a)^4}sg_bg_c &= N_{K_{T^2-g_a}/\mathbb{C}(x,s)}((T+S_-)(T+\beta S_-)(T+\gamma S_-)) \\ &= N_{K_{T^2-g_a}/\mathbb{C}(x,s)}(\ (g_a+(\beta\gamma+\beta+\gamma)S_-^2)T \\ &\qquad +(\beta\gamma S_-^2+(1+\beta+\gamma)g_a)S_-) \\ &= N_{K_{T^2-g_a}/\mathbb{C}(x,s)}\left(\tfrac{2d}{(1-a)^2}qT+(1+\beta)(1+\gamma)u\right), \end{aligned}$$

c'est-à-dire que

$$\frac{(1-a)^4(1+\beta)^2(1+\gamma)^2}{4d^2}u^2 = -sg_bg_c+q^2g_a.$$

Les polynômes S_- et g_a sont premiers entre eux. Les polynômes $u = \frac{(\beta\gamma S_-^2+(1+\beta+\gamma)g_a)S_-}{(1+\beta)(1+\gamma)}$ et g_a sont donc aussi premiers entre eux. Nous appliquons le théorème 2.3.1.2 : le double de $< u, v >$ est $< g_a, 0 >$.

Nous supposons maintenant l'appartenance de β et γ à $i\mathbb{R}(x)$. Soit $\check{v}$ l'unique polynôme de degré 3 tel que $\check{v} \equiv v \bmod u$ (ou de façon équivalente tel que $\check{v} \equiv qg_a \bmod u$) et $\check{v}(0) = 0$. D'après le théorème 2.2.4, la τ-invariance de $< u, v >$ s'obtient en vérifiant que

* $f-\check{v}^2 = su(s)\frac{s^{\deg(u)}}{u(0)}\sigma(u)\left(\frac{d^2}{s}\right)$,
* et $\check{v} = \frac{s^4}{d^4}\tau(\check{v})$.

Nous commençons par calculer $\check{v}$. Les polynômes g_a, et S_- sont unitaires de degrés 2 et 1 respectivement. Par conséquent, le polynôme u est unitaire de degré 3, et le polynôme q est de degré 2 et de coefficient dominant $\lambda := \frac{(1-a)^2(1+\beta)(1+\gamma)}{2d}$. Nous en déduisons que le polynôme $qg_a - \lambda uS_-$ est de degré au plus 3. De plus, comme $S_-(0) = -d$ et $g_a(0) = d^2$, le polynôme

$$qg_a - \lambda uS_- = \frac{(1-a)^2}{2d}(g_a - S_-^2)(g_a+\beta\gamma S_-^2)$$

s'annule en 0. Le polynôme $\check{v}$ est donc égal à $qg_a - \lambda uS_-$.

En appliquant les égalités $\frac{s}{d}\tau(S_-) = -S_-$ et $\frac{s^2}{d^2}\tau(g_a) = g_a$ à la formule $\check{v} = \frac{(1-a)^2}{2d}(g_a - S_-^2)(g_a+\beta\gamma S_-^2)$, nous vérifions que $\check{v} = \frac{s^4}{d^4}\tau(\check{v})$.

Pour conclure la τ-invariance de $< u, v >$, il suffit maintenant de montrer que $f-\check{v}^2 = su(s)\frac{s^{\deg(u)}}{u(0)}\sigma(u)\left(\frac{d^2}{s}\right)$.

Nous avons montré précédemment que $f = (qg_a)^2 - \lambda^2u^2g_a$. Puisque $\check{v} = qg_a - \lambda uS_-$, on a

$$\begin{aligned} f-\check{v}^2 &= (qg_a)^2 - \lambda^2u^2g_a - \check{v}^2 \\ &= (\lambda uS_- + \check{v})^2 - \lambda^2u^2g_a - \check{v}^2 \\ &= \lambda^2(S_-^2 - g_a)u^2 + 2\lambda u\check{v}S_-. \end{aligned}$$

Nous factorisons le polynôme $f - \check{v}^2$ en utilisant l'égalité $\check{v} = -\frac{(1-a)^2}{2d}(S_-^2 - g_a)(g_a + \beta\gamma S_-^2)$: on obtient

$$f - \check{v}^2 = \lambda u(S_-^2 - g_a)\left(\lambda u - 2\frac{(1-a)^2}{2d}(g_a + \beta\gamma S_-^2)S_-\right)^2. \qquad (2.10)$$

Puisque $\lambda u = \frac{(1-a)^2}{2d}((1+\beta+\gamma)g_a + \beta\gamma S_-^2)S_-$ et $(S_-^2 - g_a) = -\frac{4d}{1-a}s$ la factorisation 2.10 se réécrit :

$$f - \check{v}^2 = -2\lambda(1-a)su(s)((-1+\beta+\gamma)g_a - \beta\gamma S_-^2)S_-. \qquad (2.11)$$

Des égalités $\tau(\beta) = -\beta$, $\tau(\gamma) = -\gamma$, $s\tau(S_-) = -dS_-$ et $s^2\tau(g_a)$, nous déduisons que

$$\begin{array}{rcl} \frac{s^{\deg(u)}}{u(0)}\tau(u)(s) & = & -\left(\frac{s}{d}\right)^3 \tau\left(\frac{(\beta\gamma S_-^2 + (1+\beta+\gamma)g_a)S_-}{(1+\beta)(1+\gamma)}\right) \\ & = & -\frac{1}{(1-\beta)(1-\gamma)}((-1+\beta+\gamma)g_a - \beta\gamma S_-^2)S_-. \end{array}$$

En remplaçant dans l'égalité 2.11 on obtient

$$\begin{array}{rcl} f - \check{v}^2 & = & \frac{(1-a)^3(1-\beta^2)(1-\gamma^2)}{d}su(s)\frac{s^{\deg(u)}}{u(0)}\sigma(u)\left(\frac{d^2}{s}\right) \\ & = & su(s)\frac{s^{\deg(u)}}{u(0)}\sigma(u)\left(\frac{d^2}{s}\right) \end{array}$$

(car $d = (1-a)(1-b)(1-c)$ et $(1-\beta^2) = \frac{1-b}{1-a}$ et $(1-\gamma^2) = \frac{1-c}{1-a}$). Ainsi, d'après la proposition 2.2.4, le diviseur $\tau(\mathrm{div}(u,v)) - (\mathrm{div}(u,v)$ est le diviseur principal associé à la fonction $\frac{t+\check{v}}{su(s)} = \frac{2dt + (1-a)^2(g_a - S_-^2)(g_a + \beta\gamma S_-^2)}{2dsu(s)}$. □

Théorème 2.5.2.8 *Soient a, b, $c \in \mathbb{R}(x)$ trois fractions rationnelles positives non nulles différentes de 1 et deux à deux distinctes. On note $d := (1-a)(1-b)(1-c)$.*

On suppose que $(b-a)(1-a)$, $(c-a)(1-a)$ et $-d = (a-1)(b-1)(c-1)$ sont des carrés dans $\mathbb{R}(x)$, c'est-à-dire l'existence de trois fractions rationnelles α, β, et $\gamma \in \mathbb{R}(x)$ non nulles telles que

$$\begin{array}{l} a = 1 + \alpha^2(1+\beta^2)(1+\gamma^2), \\ b = 1 + \alpha^2(1+\beta^2)^2(1+\gamma^2) \text{ et} \\ c = 1 + \alpha^2(1+\beta^2)(1+\gamma^2)^2. \end{array}$$

Alors le polynôme $P(y) := (y^2+1)(y^2+a)(y^2+b)(y^2+c)$ est un somme de trois carrés dans $\mathbb{R}(x,y)$:

$$\begin{array}{rcl} P(y) & = & \left(\frac{(a-1)y(y^2+a)}{\alpha} + \alpha\beta\gamma((1-\beta\gamma)y + \beta + \gamma)(y^2+1)\right)^2 \\ & & + \left(\frac{(a-1)(y^2+a)}{\alpha} + \alpha\beta\gamma(1 - \beta\gamma - (\beta+\gamma)y)(y^2+1)\right)^2 \\ & & + \left((y^2+1)(y^2 + a - \beta\gamma(a-1))\right)^2. \end{array}$$

Démonstration.

La situation est celle de la proposition 2.5.2.7. On en conserve les notations. Un antécédent de $< g_a, 0 >$ pour la multiplication par 2 est le point $< u, v >$ avec

* $u := \frac{(-\beta\gamma S_-^2 + (1+i\beta+i\gamma)g_a)S_-}{(1+i\beta)(1+i\gamma)}$,
* $\check{v} := \frac{(1-a)^2}{2d}(g_a - S_-^2)(g_a - \beta\gamma S_-^2)$ et
* v le reste de la division euclidienne de $\check{v}$ par u.

Ce diviseur est τ-invariant car β et γ sont dans $\mathbb{R}(x)$.

L'évaluation du polynôme u en 0 est $-d^3 \in \mathbb{R}(x)^2$. D'après le théorème 2.2.4, le point $< u, v >$ est τ-antineutre. Par suite, le polynôme $P(y) = (y^2+1)(y^2+a)(y^2+b)(y^2+c)$ est une somme de trois carrés.

La τ-invariance de $< u, v >$ signifie que le diviseur $\tau(\mathrm{div}(u,v)) - \mathrm{div}(u,v)$ est principal. La proposition 2.5.2.7 nous précise la fonction associée : il s'agit de la fonction $h := \frac{(t+\check{v}(s))}{su(s)}$. Soit $H := \Gamma^{-1}(h)$. Comme

* $\Gamma^{-1}\left(\frac{t}{S_-^4}\right) = \frac{-iz}{2d}$,
* $\Gamma^{-1}\left(\frac{s}{S_-}\right) = \Gamma^{-1}\left(\frac{1}{2}\left(1 + \frac{s+d}{s-d}\right)\right) = \frac{y+i}{2i}$ et
* $\Gamma^{-1}\left(\frac{g_a}{S_-^2}\right) = \Gamma^{-1}\left(\frac{1}{a-1}\left(a - \left(\frac{s+d}{s-d}\right)^2\right)\right) = \frac{y^2+a}{a-1}$,

la fonction H est égale à $\frac{(-iz+2d\nu)}{-id(y+i)(\mu_1+i\mu_2)}$, avec

$$\begin{aligned}
* \quad \mu_1 &:= \mathrm{Re}\left(\Gamma^{-1}\left(\tfrac{u}{S_-^3}\right)\right) \\
&= \mathrm{Re}\left(\Gamma^{-1}\left(\tfrac{-\beta\gamma}{(1+i\beta)(1+i\gamma)} + \left(1 + \tfrac{\beta\gamma}{(1+i\beta)(1+i\gamma)}\right)\tfrac{g_a}{S_-^2}\right)\right) \\
&= \mathrm{Re}\left(\tfrac{-\beta\gamma}{(1+i\beta)(1+i\gamma)} + \left(1 + \tfrac{\beta\gamma}{(1+i\beta)(1+i\gamma)}\right)\tfrac{y^2+a}{a-1}\right) \\
&= \mathrm{Re}\left(\tfrac{y^2+a}{a-1} + \tfrac{\beta\gamma}{(1+i\beta)(1+i\gamma)}\tfrac{y^2+1}{a-1}\right) \\
&= \tfrac{y^2+a}{a-1} + \tfrac{\beta\gamma(1-\beta\gamma)}{(1+\beta^2)(1+\gamma^2)}\tfrac{y^2+1}{a-1},
\end{aligned}$$

$$\begin{aligned}
* \quad \mu_2 &:= \mathrm{Im}\left(\Gamma^{-1}\left(\tfrac{u}{S_-^3}\right)\right) \\
&= -\tfrac{\beta\gamma(\beta+\gamma)}{(1+\beta^2)(1+\gamma^2)}\tfrac{y^2+1}{a-1} \text{ et}
\end{aligned}$$

$$\begin{aligned}
* \quad \nu &:= \Gamma^{-1}\left(\tfrac{\check{v}}{S_-^4}\right) \\
&= \Gamma^{-1}\left(\tfrac{(1-a)^2}{2d}\left(\tfrac{g_a}{S_-^2} - 1\right)\left(\tfrac{g_a}{S_-^2} - \beta\gamma\right)\right) \\
&= \tfrac{(y^2+1)(y^2+a-\beta\gamma(a-1))}{2d},
\end{aligned}$$

c'est-à-dire égale à $(a_1 + tb_1) + i(a_2 + tb_2)$ avec

* $b_1 := \frac{y\mu_1 - \mu_2}{d(y^2+1)(\mu_1^2+\mu_2^2)}$, $a_2 := -2d\nu b_1$,
* $b_2 := -\frac{\mu_1 + y\mu_2}{d(y^2+1)(\mu_1^2+\mu_2^2)}$ et $a_1 := 2d\nu b_2$.

Nous utilisons le théorème 2.2.4 afin d'écrire -1 comme somme de deux

carrés dans le corps $\mathbb{R}(x,y)[z]/(z^2+P(y))$:

$$\begin{aligned}(a_1+b_1t)^2+(a_2+b_2t)^2 &= H\sigma(H)\\ &= \Gamma^{-1}(h\tau(h))\\ &= \tfrac{-d^2}{u(0)}\\ &= \tfrac{1}{d}\\ &= -\left(\tfrac{\alpha}{(a-1)^2}\right)^2.\end{aligned}$$

D'après le lemme 1.2.4, on a donc

$$P(y) = \left(\tfrac{\alpha}{(a-1)^2}\tfrac{b_1}{(b_1^2+b_2^2)}\right)^2+\left(\tfrac{\alpha}{(a-1)^2}\tfrac{b_2}{(b_1^2+b_2^2)}\right)^2+\left(\tfrac{b_1a_2-b_2a_1}{b_1^2+b_2^2}\right)^2.$$

On conclue en remarquant que $b_1^2+b_2^2 = \frac{1}{d^2(y^2+1)(\mu_1^2+\mu_2^2)}$ et $b_2a_1-b_1a_2 = 2d\nu(b_1^2+b_2^2)$: on a donc

$$\begin{aligned}\tfrac{b_1}{b_1^2+b_2^2} &= d(y\mu_1-\mu_2)\\ &= d\left(\tfrac{y(y^2+a)}{a-1}+\tfrac{\beta\gamma}{(1+\beta^2)(1+\gamma^2)(a-1)}(y^2+1)((1-\beta\gamma)y+\beta+\gamma)\right),\\ \tfrac{b_2}{b_1^2+b_2^2} &= -d(\mu_1+y\mu_2)\\ &= -d\left(\tfrac{(y^2+a)}{a-1}+\tfrac{\beta\gamma}{(1+\beta^2)(1+\gamma^2)(a-1)}(y^2+1)(1-\beta\gamma-(\beta+\gamma)y)\right) \text{ et}\\ \tfrac{b_2a_1-b_1a_2}{b_1^2+b_2^2} &= 2d\nu\\ &= (y^2+1)(y^2+a-\beta\gamma(a-1)).\quad \square\end{aligned}$$

Chapitre 3

La méthode de calcul du rang de Mordell-Weil.

À partir de maintenant, nous nous intéressons à des polynômes sans facteur carré de la forme

$$P(y) = (y^2+1)(y^2+C(x^2))(y^4+(1+C(x^2))y^2+B(x^2))$$

où B, $C \in \mathbb{R}[x]$ sont des polynômes totalement positifs. La proposition 1.2.8 affirme que le polynôme $P(y)$ est une somme de trois carrés si et seulement si la jacobienne de la courbe hyperelliptique $\mathcal{C}$ d'équation affine $z^2 + P(y) = 0$ a un $\mathbb{R}(x)$-point antineutre. L'existence de points de torsion 2-primaire antineutres a déjà été discutée au cours de la section 2.4. L'étape suivante dans notre étude est de montrer que le $\mathbb{R}(x)$-rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})$ est nul.

Dans ce chapitre, nous relions une étude de l'image de certains morphismes de Cassels-Schaefer à l'étude de la nullité du $\mathbb{R}(x)$-rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})$. Plus précisément, nous expliquons comment la forme particulière de P permet d'obtenir des isogénies entre $\mathrm{Jac}(\mathcal{C})$ et des jacobiennes plus simples. Nous effectuons aussi une 2-descente : nous pouvons ainsi calculer des rangs de Mordell-Weil sur $\mathbb{R}(x)$ à l'aide de rangs de Mordell-Weil sur un corps de la forme $k(x)$, le corps k étant une extension de $\mathbb{Q}$ mieux adaptée que $\mathbb{R}$ aux calculs de rangs de Mordell-Weil.

3.1 L'existence des rangs de Mordell-Weil.

Au cours de ce chapitre, nous allons étudier le rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$. Nous devons au préalable vérifier que ce rang de Mordell-Weil est bien défini. Pour cela nous utilisons le théorème de Lang-Néron.

Théorème 3.1.1 (Lang, Néron) *Soient k un corps et F le corps de fonction d'une variété définie sur k. Soit A une variété abélienne sur F. Nous*

supposons qu'il n'existe aucune sous-variété abélienne B de A qui provienne d'une variété abélienne de dimension au moins 1 définie sur k. Alors le groupe abélien $A(F)$ est de type fini.

Démonstration.
Le lecteur se reportera à [Lan97] page 27 théorème 4.2. □

Corollaire 3.1.2 *Soit k_0 un sous-corps de $\mathbb{C}$. Soient $f \in k_0(x)[y]$ un polynôme de degré impair et $\mathcal{C}$ la courbe hyperelliptique sur $k_0(x)$ d'équation affine $z^2 = f(y)$. Soit J la jacobienne de $\mathcal{C}$. Nous supposons que la torsion 2-primaire de $J(\mathbb{C}(x))$ est finie.*

Le groupe $J(\mathbb{C}(x))$ est alors abélien de type fini.

Démonstration.
Supposons qu'il existe une sous-variété abélienne A de dimension au moins 1 de la jacobienne J qui provienne d'une variété abélienne définie sur $\mathbb{C}$. La torsion 2-primaire de $A(\mathbb{C})$ est de cardinal infini car $\mathbb{C}$ est algébriquement clos. Par suite, la torsion 2-primaire de $A(\mathbb{C}(x))$ est aussi de cardinal infini. Cela contredit l'hypothèse selon laquelle la torsion 2-primaire de $J(\mathbb{C}(x))$ est finie. Ainsi, J n'admet aucune sous-variété abélienne de dimension au moins 1 qui provienne d'une variété abélienne définie sur $\mathbb{C}$. Nous sommes donc sous les hypothèses du théorème 3.1.1 et le groupe $J(\mathbb{C}(x))$ est de type fini. □

Corollaire 3.1.3 *Soient B et C deux éléments de $\mathbb{R}(x)$. Soit $\mathcal{C}$ la courbe hyperelliptique d'équation affine*

$$z^2 + (y^2+1)(y^2 + C(x^2))(y^4 + (1 + C(x^2))y^2 + B(x^2)) = 0.$$

Soit J la jacobienne de la courbe $\mathcal{C}$. Nous supposons que $B(x^2)$, $C(x^2)$, $B(x^2)C(x^2)$, $B(x^2) - C(x^2)$, $(B(x^2) - C(x^2))(1 - C(x^2))$ et $(1 + C(x^2))^2 - 4B(x^2)$ ne sont pas des carrés dans $\mathbb{C}(x)$.

Alors le groupe $J(\mathbb{C}(x))$ est de type fini.

Démonstration.
D'après le corollaire 2.4.8, la torsion 2-primaire $J(\mathbb{C}(x))$ est de cardinal fini. Par conséquent, la courbe $\mathcal{C}$ satisfait aux conditions du corollaire 3.1.2. Le groupe $J(\mathbb{C}(x))$ est donc bien de type fini. □

3.2 Une décomposition du problème

Notations 3.2.1 *Soit F un corps de fonction. Soit F_2 une extension finie de F. Soit $\mathfrak{p}$ une place de F et $\mathfrak{P}$ une place de F_2 au dessus de $\mathfrak{p}$. Nous notons alors $e(\mathfrak{P}|\mathfrak{p})$ l'indice de ramification de $\mathfrak{P}$ au dessus de $\mathfrak{p}$ et $f(\mathfrak{P}|\mathfrak{p}) := [\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} : \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}]$ le degré résiduel de $\mathfrak{P}$ au dessus de $\mathfrak{p}$.*

Définition 3.2.2 *Nous conservons les notations 3.2.1. À toute place* $\mathfrak{p}$ *de* F *nous associons sa conorme (relative à* F_2/F*) : nous posons*

$$Cn_{F_2/F}(\mathfrak{p}) = \sum_{\mathcal{P} \text{ place de } F_2,\ \mathcal{P}|\mathfrak{p}} e(\mathcal{P}|\mathfrak{p})\mathcal{P} \in Div(F_2).$$

Nous définissons ainsi par linéarité un morphisme $Cn_{F_2/F}$ *du groupe* $Div^0(F)$ *vers le groupe* $Div^0(F_2)$.

L'image d'un diviseur principal par le morphisme $Cn_{F_2/F}$ *est un diviseur principal de* F_2 *(voir* [Sti93] *Proposition III.1.9). Par conséquent,* $Cn_{F_2/F}$ *induit un morphisme de groupe* $CN_{F_2/F} : Pic^0(F) \longrightarrow Pic^0(F_2)$.

Lemme 3.2.3 *Soit* k *un corps de caractéristique* 0. *Soient* $P(T) \in k[T]$ *et* $\mathcal{C}$ *la courbe hyperelliptique sur* k *d'équation affine* $z^2 + P(y) = 0$. *Soit* $\rho : k(\mathcal{C}) \longrightarrow k(\mathcal{C})$ *une involution différente de l'identité. Soit* $D \in Div^0(k(\mathcal{C})^\rho)$ *un diviseur de degré* 0.

Alors le diviseur $Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(D)$ *est* ρ*-invariant.*

Démonstration.

Le corps k est parfait (car de caractéristique 0). Puisque ρ est une involution différente de l'identité, l'extension $k(\mathcal{C})/k(\mathcal{C})^\rho$ est de degré 2. Son groupe de Galois est donc de degré au plus 2. Ce groupe de Galois contient ρ donc $\mathrm{Gal}(k(\mathcal{C})/k(\mathcal{C})^\rho = \{\mathrm{Id}, \rho\}$ et l'extension $k(\mathcal{C})/k(\mathcal{C})^\rho$ est galoisienne.

Puisque le morphisme $Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}$ est obtenu par linéarité, il suffit, pour montrer le lemme, de vérifier que $Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(\mathfrak{p})$ est ρ-invariant pour toute place $\mathfrak{p}$ de $k(\mathcal{C})^\rho$.

Soit $\mathfrak{p}$ une place de $k(\mathcal{C})^\rho$. Pour toute place $\mathcal{P}$ au dessus de $\mathfrak{p}$, les indices de ramification $e(\mathcal{P}|\mathfrak{p})$ et $e(\rho(\mathcal{P})|\mathfrak{p})$ sont égaux (voir par exemple [Sti93] Lemme III.5.2). Par conséquent, l'image de $Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(\mathfrak{p})$ par ρ est

$$\begin{aligned} \rho\left(Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(\mathfrak{p})\right) &= \sum_{\mathcal{P} \text{ place de } k(\mathcal{C}),\ \mathcal{P}|\mathfrak{p}} e(\mathcal{P}|\mathfrak{p})\rho(\mathcal{P}) \\ &= \sum_{\mathcal{P} \text{ place de } k(\mathcal{C}),\ \mathcal{P}|\mathfrak{p}} e(\rho(\mathcal{P})|\mathfrak{p})\rho(\mathcal{P}). \end{aligned}$$

L'extension $k(\mathcal{C})/k(\mathcal{C})^\rho$ étant galoisienne, ρ agit transitivement sur l'ensemble des places de $k(\mathcal{C})$ au dessus de $\mathfrak{p}$ (voir [Sti93] Théorème III.7.1). Nous avons ainsi

$$\begin{aligned} \rho\left(Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(\mathfrak{p})\right) &= \sum_{\mathcal{P} \text{ place de } k(\mathcal{C}),\ \mathcal{P}|\mathfrak{p}} e(\rho(\mathcal{P})|\mathfrak{p})\rho(\mathcal{P}). \\ &= \sum_{\mathcal{P} \text{ place de } k(\mathcal{C}),\ \mathcal{P}|\mathfrak{p}} e(\mathcal{P}|\mathfrak{p})\mathcal{P} \\ &= Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(\mathfrak{p}). \quad \square \end{aligned}$$

Lemme 3.2.4 *Soit k un corps de caractéristique 0. Soient $P(T) \in k[T]$ et $\mathcal{C}$ la courbe hyperelliptique sur k d'équation affine $z^2 + P(y) = 0$. Soit $\rho : k(\mathcal{C}) \longrightarrow k(\mathcal{C})$ une involution différente de l'identité.*

Alors le noyau de l'homomorphisme $CN_{k(\mathcal{C})/k(\mathcal{C})^\rho}$ est contenu dans la 2-torsion de $Pic^0(k(\mathcal{C})^\rho)$.

Démonstration.

Soit $D \in \mathrm{Div}^0(k(\mathcal{C})^\rho)$ un diviseur tel que $Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(D)$ soit un diviseur principal. Soit $f \in k(\mathcal{C})$ une fonction telle que $Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(D) = \mathrm{div}(f)$. D'après le lemme 3.2.3, le diviseur $Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(D)$ est ρ-invariant. Nous en déduisons

$$\begin{aligned} Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(2D) &= 2Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(D) \\ &= Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(D) + \rho(Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}(D)) \\ &= \mathrm{div}(f) + \rho(\mathrm{div}(f) \\ &= \mathrm{div}(f\rho(f)). \end{aligned}$$

Puisque la fonction $f\rho(f)$ est un élément de $k(\mathcal{C})^\rho$, le diviseur $\mathrm{div}(f\rho(f)) \in \mathrm{Div}^0(k(\mathcal{C}))$ est l'image par $Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}$ du diviseur principal $\mathrm{div}(f\rho(f))) \in \mathrm{Div}^0(k(\mathcal{C})^\rho)$ (voir [Sti93] Théorème III.1.9). Ainsi, le morphisme $Cn_{k(\mathcal{C})/k(\mathcal{C})^\rho}$ étant injectif, $2D$ est le diviseur principal de $k(\mathcal{C})^\rho$ associé à la fonction $f\rho(f)$. En particulier, la classe d'équivalence linéaire de D est un élément de 2-torsion de $Pic^0(k(\mathcal{C})^\rho)$. □

Lemme 3.2.5 *Soit k un corps de caractéristique 0. Soient $P(T) \in k[T]$ et $\mathcal{C}$ la courbe hyperelliptique sur k d'équation affine $z^2 + P(y) = 0$. Soient $\iota : \begin{array}{ccc} k(\mathcal{C}) & \longrightarrow & k(\mathcal{C}) \\ A(y,z) & \longmapsto & A(y,-z) \end{array}$ l'involution hyperelliptique et $\rho : k(\mathcal{C}) \longrightarrow k(\mathcal{C})$ une involution différente de l'identité et de ι. Nous supposons que ι et ρ commutent.*

Alors l'homomorphisme $+ \circ \left(CN_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}} \times CN_{k(\mathcal{C})/k(\mathcal{C})^\rho}\right)$ est de noyau fini.

Démonstration.

Soit $(\alpha_\rho, \alpha_{\iota\circ\rho}) \in \mathrm{Pic}^0(k(\mathcal{C})^\rho) \times \mathrm{Pic}^0(k(\mathcal{C})^{\iota\circ\rho})$. D'après le lemme 3.2.3,

* l'élément $CN_{k(\mathcal{C})/k(\mathcal{C})^\rho}(\alpha_\rho)$ est invariant sous ρ, et
* l'élément $CN_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}}(\alpha_{\iota\circ\rho})$ est invariant sous $\iota \circ \rho$.

Nous supposons que $CN_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}}(\alpha_{\iota\circ\rho}) + CN_{k(\mathcal{C})/k(\mathcal{C})^\rho}(\alpha_\rho) = 0$. L'élément $CN_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}}(\alpha_{\iota\circ\rho}) = -CN_{k(\mathcal{C})/k(\mathcal{C})^\rho}(\alpha_\rho)$ est alors ρ-invariant et $(\iota \circ \rho)$-invariant. Par suite, il est ι-invariant, c'est-à-dire qu'il est de 2-torsion. Les images $CN_{k(\mathcal{C})/k(\mathcal{C})^\rho}(2\alpha_\rho)$ et $CN_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}}(2\alpha_{\iota\circ\rho})$ sont donc triviales.

Nous appliquons maintenant le lemme 3.2.4 aux deux involutions ρ et $\iota \circ \rho$:

* le noyau de l'homomorphisme $CN_{k(\mathcal{C})/k(\mathcal{C})^\rho}$ est contenu dans la 2-torsion de $\mathrm{Pic}^0(k(\mathcal{C})^\rho)$, et
* le noyau de l'homomorphisme $CN_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}}$ est contenu dans la 2-torsion de $\mathrm{Pic}^0(k(\mathcal{C})^{\iota\circ\rho})$.

Ainsi, les éléments α_ρ et $\alpha_{\iota\circ\rho}$ sont de 4-torsion.

Soit F un corps de fonctions sur un corps K. Par définition, il existe un élément $s \in F$ transcendant sur K tel que F soit une extension algébrique finie de $K(s)$. Le corps de fonctions F est donc le corps de fonctions d'une courbe $\mathcal{D}$ définie sur K. Le groupe $\mathrm{Pic}^0(F)$ est un sous-groupe du groupe $\mathrm{Jac}(\mathcal{D})(K)$. Or la 4-torsion de $\mathrm{Jac}(\mathcal{D})(K)$ est de cardinal fini, donc la 4-torsion du groupe $\mathrm{Pic}^0(F)$ est de cardinal fini.

Nous appliquons cette remarque au corps $F = k(\mathcal{C})^\rho$, puis au corps $F = k(\mathcal{C})^{\iota\circ\rho}$: la 4-torsion de $\mathrm{Pic}^0(k(\mathcal{C})^\rho)$ et la 4-torsion de $\mathrm{Pic}^0(k(\mathcal{C})^{\iota\circ\rho})$ sont de cardinal fini. Par conséquent, l'homomorphisme

$$+ \circ \left(CN_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}} \times CN_{k(\mathcal{C})/k(\mathcal{C})^\rho}\right)$$

est bien de noyau fini. □

Proposition 3.2.6 *Soit k un corps de caractéristique 0. Soient $P(T) \in k[T]$ et $\mathcal{C}$ la courbe hyperelliptique sur k d'équation affine $z^2 + P(y) = 0$. Soient $\iota : \begin{array}{ccc} k(\mathcal{C}) & \longrightarrow & k(\mathcal{C}) \\ A(y,z) & \longmapsto & A(y,-z) \end{array}$ l'involution hyperelliptique et $\rho : k(\mathcal{C}) \longrightarrow k(\mathcal{C})$ une involution différente de l'identité et de ι. Nous supposons que ι et ρ commutent.*

Alors l'homomorphisme $+ \circ \left(CN_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}} \times CN_{k(\mathcal{C})/k(\mathcal{C})^\rho}\right)$ est de noyau fini et son image contient $2Pic^0(k(\mathcal{C}))$.

Démonstration.

Le corps k est parfait (car de caractéristique 0). Puisque ρ est une involution différente de l'identité, l'extension $k(\mathcal{C})/k(\mathcal{C})^\rho$ est de degré 2. Son groupe de Galois est donc de degré au plus 2. Ce groupe de Galois contient ρ donc $\mathrm{Gal}(k(\mathcal{C})/k(\mathcal{C})^\rho = \{\mathrm{Id}, \rho\}$ et l'extension $k(\mathcal{C})/k(\mathcal{C})^\rho$ est galoisienne. Par symétrie du rôle de ρ et $\iota \circ \rho$, l'extension $k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}$ est galoisienne de groupe de galois $\{Id, \iota \circ \rho\}$.

Soit $\mathcal{P}$ une place de $k(\mathcal{C})$. Alors $\mathfrak{p} := \mathcal{P} \cap k(\mathcal{C})^{\iota\circ\rho}$ est une place de $k(\mathcal{C})^{\iota\circ\rho}$. Les places de $k(\mathcal{C})$ au dessus de $\mathfrak{p}$ sont $\mathcal{P}$ et $(\iota\circ\rho)(\mathcal{P})$ (voir [Sti93] Proposition III.7.1).

Si les places $\mathcal{P}$ et $(\iota\circ\rho)(\mathcal{P})$ sont distinctes, alors l'extension $k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}$ n'est ramifiée ni en $\mathcal{P}$ ni en $(\iota\circ\rho)(\mathcal{P})$ (l'extension $k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}$ est de degré 2). Dans ce cas, $\mathcal{P} + (\iota \circ \rho)(\mathcal{P}) = Cn_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}}(\mathfrak{p})$ est dans l'image de $Cn_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}}$.

Nous reprenons les notations 3.2.1. Nous traitons le cas où $\mathcal{P} = (\iota\circ\rho)(\mathcal{P})$ en utilisant la formule $\sum_{\mathfrak{P} \text{ place de } k(\mathcal{C}),\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p}) = 2$ (voir [Sti93] Théorème III.1.11). Lorsque $\mathcal{P} = (\iota\circ\rho)(\mathcal{P})$, la place $\mathcal{P}$ est la seule place au dessus de $\mathfrak{p}$ et donc

$$\begin{aligned} \mathcal{P} + (\iota\circ\rho)(\mathcal{P}) &= 2\mathcal{P} \\ &= e(\mathcal{P}|\mathfrak{p})f(\mathcal{P}|\mathfrak{p})\mathcal{P} \\ &= Cn_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}}(f(\mathcal{P}|\mathfrak{p})\mathfrak{p}) \end{aligned}$$

Ainsi, le diviseur $\mathcal{P} + (\iota\circ\rho)(\mathcal{P})$ est dans l'image de $Cn_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}}$.

La situation est la même lorsque nous remplaçons l'involution ρ par l'involution $\iota\circ\rho$. Ainsi le diviseur $\mathcal{P} + \rho(\mathcal{P})$ est dans l'image de $Cn_{k(\mathcal{C})/k(\mathcal{C})^{\rho}}$.

L'application $+\circ\left(Cn_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}} \times Cn_{k(\mathcal{C})/k(\mathcal{C})^{\rho}}\right)$ est un morphisme de groupe et son image contient tous les diviseurs de la forme $2\mathcal{P} + \rho(\mathcal{P}) + \iota(\rho(\mathcal{P}))$ avec $\mathcal{P}$ une place de $k(\mathcal{C})$. Son image contient donc aussi tous les diviseurs de la forme $2D+\rho(D)+\iota(\rho(D))$ avec $D \in \mathrm{div}^0(k(\mathcal{C}))$. Or pour tout diviseur $D \in \mathrm{div}^0(k(\mathcal{C}))$, le diviseur $2D + \rho(D) + \iota(\rho(D))$ est linéairement équivalent à $2D$, donc le groupe $2\mathrm{Pic}^0(k(\mathcal{C}))$ est contenu dans l'image de $+\circ\left(CN_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}} \times CN_{k(\mathcal{C})/k(\mathcal{C})^{\rho}}\right)$.

Pour conclure nous faisons appel au lemme 3.2.5 : l'homomorphisme $+\circ\left(CN_{k(\mathcal{C})/k(\mathcal{C})^{\iota\circ\rho}} \times CN_{k(\mathcal{C})/k(\mathcal{C})^{\rho}}\right)$ est de noyau fini. □

Proposition 3.2.7 *Soit k un corps de caractéristique 0. Soient $P(T) \in k[T]$ et $\mathcal{C}$ la courbe hyperelliptique sur k d'équation affine $z^2 + P(y^2) = 0$.*

Nous notons $\mathcal{C}^+$ et $\mathcal{C}^-$ les k-courbes hyperelliptiques d'équations affines respectives :

$$\mathcal{C}^+ : t^2 + sP(s) = 0 \text{ et}$$
$$\mathcal{C}^- : \beta^2 + P(\alpha) = 0.$$

Il existe alors un morphisme de groupe de $Pic^0(k(\mathcal{C}^+)) \times Pic^0(k(\mathcal{C}^-))$ vers $Pic^0(k(\mathcal{C}))$ de noyau fini et dont l'image contient $2Pic^0(k(\mathcal{C}))$.

Si de plus la courbe $\mathcal{C}$ a un point k-rationnel, alors la jacobienne $Jac(\mathcal{C})$ est isogène sur k au produit $Jac(\mathcal{C}^+) \times Jac(\mathcal{C}^-)$.

Démonstration.

Nous considérons l'involution hyperelliptique $\iota : \begin{array}{ccc} k(\mathcal{C}) & \longrightarrow & k(\mathcal{C}) \\ A(y,z) & \longmapsto & A(y,-z) \end{array}$ et l'involution $\rho : \begin{array}{ccc} k(\mathcal{C}) & \longrightarrow & k(\mathcal{C}) \\ A(y,z) & \longmapsto & A(-y,z) \end{array}$. Nous présentons les sous-corps

$k(\mathcal{C})^\rho$ et $k(\mathcal{C})^{\iota\circ\rho}$ comme les corps de fonctions de $\mathcal{C}^-$ et $\mathcal{C}^+$ grâce aux deux morphismes

$$\begin{array}{rccccc} \phi^+ : & k(\mathcal{C}^+) & \longrightarrow & k(\mathcal{C}) & \text{et } \phi^- : & k(\mathcal{C}^-) & \longrightarrow & k(\mathcal{C}) \\ & A(s,t) & \longmapsto & A(y^2, yz) & & A(s,t) & \longmapsto & A(y^2, z) \end{array} .$$

Puisque les morphismes $\iota \circ \rho \circ \phi^+$ et ϕ^+ sont égaux, l'image de ϕ^+ est un sous-corps de $k(\mathcal{C})^{\iota\circ\rho}$. Or $k(\mathcal{C})$ est une extension de degré 2 de $\mathrm{Im}(\phi^+)$, donc l'image de ϕ^+ est $k(\mathcal{C})^{\iota\circ\rho}$. De même, $\rho \circ \phi^- = \phi^-$, donc l'image de ϕ^- est $k(\mathcal{C})^\rho$.

Nous faisons maintenant appel à la proposition 3.2.6 : le morphisme de groupe

$$+\circ\big(CN_{k(\mathcal{C})/k(\mathcal{C}^+)} \times CN_{k(\mathcal{C})/k(\mathcal{C}^-)}\big) : \mathrm{Pic}^0(k(\mathcal{C}^+)) \times \mathrm{Pic}^0(k(\mathcal{C}^-)) \longrightarrow \mathrm{Pic}^0(k(\mathcal{C}))$$

est de noyau fini et son image contient $2\mathrm{Pic}^0(k(\mathcal{C}))$. Ceci montre la première assertion de la proposition.

Nous supposons maintenant que la courbe $\mathcal{C}$ a un point k-rationnel. Les morphismes $\phi^+ : k(\mathcal{C}^+) \longrightarrow k(\mathcal{C})$ et $\phi^- : k(\mathcal{C}^+) \longrightarrow k(\mathcal{C})$ sont des morphismes de k-algèbres. Ils induisent donc deux revêtements $\Phi^+ : \mathcal{C} \longrightarrow \mathcal{C}^+$ et $\Phi^- : \mathcal{C} \longrightarrow \mathcal{C}^-$ de degré 2 définis sur k. Nous avons supposé que la courbe $\mathcal{C}$ a un point k-rationnel. Par suite, les courbes $\mathcal{C}^+$ et $\mathcal{C}^-$ possèdent toutes deux un point k-rationnel. Les trois assertions suivantes sont donc vérifiées :

* les morphismes Φ^+ et Φ^- induisent deux morphismes de schémas en groupe $\Phi^{+*} : \mathrm{Jac}(\mathcal{C}^+) \longrightarrow \mathrm{Jac}(\mathcal{C})$ et $\Phi^{-*} : \mathrm{Jac}(\mathcal{C}^-) \longrightarrow \mathrm{Jac}(\mathcal{C})$,
* pour toute extension K de k, nous avons un isomorphisme de groupes $\Psi_K^+ : \mathrm{Pic}^0(K(\mathcal{C}^+)) \longrightarrow \mathrm{Jac}(\mathcal{C}^+)(K)$ tel que l'application induite par Φ^{+*} sur $\mathrm{Jac}(\mathcal{C}^+)(K)$ soit $\Psi_K^+ \circ CN_{K(\mathcal{C})/K(\mathcal{C}^+)} \circ (\Psi_K^+)^{-1}$, et
* pour toute extension K de k, nous avons un isomorphisme de groupe $\Psi_K^- : \mathrm{Pic}^0(K(\mathcal{C}^-)) \longrightarrow \mathrm{Jac}(\mathcal{C}^-)(K)$ tel que l'application induite par Φ^{-*} sur $\mathrm{Jac}(\mathcal{C}^-)(K)$ soit $\Psi_K^- \circ CN_{K(\mathcal{C})/K(\mathcal{C}^-)} \circ (\Psi_K^-)^{-1}$.

De la première assertion de la proposition nous déduisons donc que le morphisme de schémas en groupe $+ \circ (\Phi^{+*} \times \Phi^{-*})$ est une isogénie (définie sur k). $\square$

Corollaire 3.2.8 *Soient B, $C \in \mathbb{R}(x)$ deux fractions rationnelles, et $\mathcal{C}$ la $\mathbb{R}(x)$-courbe hyperelliptique d'équation affine*

$$\mathcal{C} : z^2 + (y^2+1)(y^2 + C(x^2))(y^4 + (1 + C(x^2))y^2 + B(x^2)) = 0.$$

Nous supposons que $B(x^2)$, $C(x^2)$, $B(x^2)C(x^2)$, $B(x^2) - C(x^2)$, $(B(x^2) - C(x^2))(1 - C(x^2))$ et $(1 + C(x^2))^2 - 4B(x^2)$ ne sont pas des carrés dans $\mathbb{C}(x)$.

Nous notons $\mathcal{C}^+$ et $\mathcal{C}^-$ les $\mathbb{R}(x)$-courbes hyperelliptiques d'équations affines respectives :

$$\mathcal{C}^+ : \beta^2 = \alpha(\alpha-1)(\alpha - C(x^2))\left(\alpha^2 - [1+C(x^2)]\alpha + B(x^2)\right) \text{ et}$$
$$\mathcal{C}^- : t^2 = s\left(s^2 - [(1-C(x^2))^2 - 2(B(x^2)-C(x^2))]s + (B(x^2)-C(x^2))^2\right).$$

Alors le $\mathbb{R}(x)$-rang de Mordell-Weil de Jac($\mathcal{C}$) est la somme des $\mathbb{R}(x)$-rang de Mordell-Weil de Jac($\mathcal{C}^+$) et Jac($\mathcal{C}^-$).

Démonstration.

Soit $\mathcal{D}$ une courbe projective lisse géométriquement intègre de genre impair, $\mathcal{D}' := \mathcal{D} \times_{\mathrm{Spec}(\mathbb{R}(x))} \mathrm{Spec}(\mathbb{C}(x))$ sa complexifiée et $\Sigma := \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Nous supposons que $\mathcal{D}'$ a un point $\mathbb{C}(x)$-rationnel. D'après la proposition 1.1, nous avons une suite exacte

$$0 \longrightarrow \mathrm{Pic}^0(\mathbb{R}(x)(\mathcal{D})) \longrightarrow \mathrm{Pic}^0\left(\mathbb{C}(x)(\mathcal{D}')\right)^{\Sigma} \xrightarrow{\delta} H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times}) \longrightarrow 0.$$

De plus, le groupe $H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times})$ est d'exposant 2. Par conséquent, le noyau $\mathrm{Pic}^0(\mathbb{R}(x)(\mathcal{D}))$ de δ contient $2\mathrm{Pic}^0(\mathbb{C}(x)(\mathcal{D}'))^{\Sigma}$. Ainsi, puisque $\mathrm{Jac}(\mathcal{D})(\mathbb{R}(x)) = \mathrm{Pic}^0(\mathbb{C}(x)(\mathcal{D}'))^{\Sigma}$ (la courbe $\mathcal{D}'$ a un point $\mathbb{C}(x)$-rationnel), nous avons les deux inclusions suivantes :

$$2\mathrm{Jac}(\mathcal{D})(\mathbb{R}(x)) \subset \mathrm{Pic}^0(\mathbb{R}(x)(\mathcal{D})) \subset \mathrm{Jac}(\mathcal{D})(\mathbb{R}(x)). \tag{3.1}$$

Soient $\mathcal{H}$ la $\mathbb{R}(x)$-courbe hyperelliptique de genre 2 d'équation affine

$$\mathcal{H} : z^2 + y(y+1)(y+C(x^2))(y^2 + (1+C(x^2))y + B(x^2)) = 0$$

et $\mathcal{E}$ la courbe elliptique sur $\mathbb{R}(x)$ d'équation affine

$$\mathcal{E} : z^2 + (y+1)(y+C(x^2))(y^2 + (1+C(x^2))y + B(x^2)) = 0.$$

D'après la proposition 3.2.7, il existe un morphisme de groupes

$$\varphi : \mathrm{Pic}^0(\mathbb{R}(x)(\mathcal{H})) \times \mathrm{Pic}^0(\mathbb{R}(x)(\mathcal{E})) \longrightarrow \mathrm{Pic}^0(\mathbb{R}(x)(\mathcal{C}))$$

de noyau fini et dont l'image contient $2\mathrm{Pic}^0(\mathbb{R}(x)(\mathcal{C}))$.

Nous appliquons les inclusions 3.1, pour $\mathcal{D} = \mathcal{H}$, pour $\mathcal{D} = \mathcal{E}$ et pour $\mathcal{D} = \mathcal{C}$. Nous obtenons respectivement les inclusions

* $2\mathrm{Jac}(\mathcal{H})(\mathbb{R}(x)) \subset \mathrm{Pic}^0(\mathbb{R}(x)(\mathcal{H})) \subset \mathrm{Jac}(\mathcal{H})(\mathbb{R}(x))$,
* $2\mathrm{Jac}(\mathcal{E})(\mathbb{R}(x)) \subset \mathrm{Pic}^0(\mathbb{R}(x)(\mathcal{E})) \subset \mathrm{Jac}(\mathcal{E})(\mathbb{R}(x))$ et
* $2\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x)) \subset \mathrm{Pic}^0(\mathbb{R}(x)(\mathcal{C})) \subset \mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$.

L'homomorphisme φ induit donc par restriction un morphisme de groupe de $2\mathrm{Jac}(\mathcal{H})(\mathbb{R}(x)) \times 2\mathrm{Jac}(\mathcal{E})(\mathbb{R}(x))$ vers $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ de noyau fini et dont l'image contient $8\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$. En particulier, le rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est la somme des rangs de Mordell-Weil de $\mathrm{Jac}(\mathcal{H})(\mathbb{R}(x))$ et

$\mathrm{Jac}(\mathcal{E})(\mathbb{R}(x))$.

L'application $\begin{array}{ccc} k(\mathcal{C}^+) & \longrightarrow & k(\mathcal{H}) \\ A(\alpha,\beta) & \longmapsto & A(-y,z) \end{array}$ induit un isomorphisme entre les courbes hyperelliptiques $\mathcal{C}^+$ et $\mathcal{H}$.

Pour montrer le corollaire 3.2.8 il suffit maintenant de voir que les courbes elliptiques $\mathcal{E}$ et $\mathcal{C}^-$ sont birationnellement équivalentes. Dans un premier temps, nous considérons la courbe elliptique $\mathcal{E}_2$ d'équation affine

$$\mathcal{E}_2 : -\tilde{z}^2 = ((C(x^2)-1)\tilde{y}+1)((B(x^2)-C(x^2))\tilde{y}^2+(C(x^2)-1)\tilde{y}+1).$$

Le morphisme $\begin{array}{ccc} k(\mathcal{E}_2) & \longrightarrow & k(\mathcal{E}) \\ A(\tilde{y},\tilde{z}) & \longmapsto & A(\frac{1}{y+1},\frac{z}{(y+1)^2}) \end{array}$ induit une équivalence birationnelle entre les courbes elliptiques $\mathcal{E}$ et $\mathcal{E}_2$.
Nous effectuons un deuxième changement de variable : nous posons

$$\begin{cases} s := -(B(x^2)-C(x^2))[(C(x^2)-1)\tilde{y}+1]. \\ t := (B(x^2)-C(x^2))(1-C(x^2))\tilde{z} \end{cases}$$

Nous montrons ainsi que $\mathcal{E}_2$ est isomorphe à la courbe elliptique $\mathcal{C}^-$. $\square$

Proposition 3.2.9 *Soit k un corps de caractéristique 0 et $f(x,y) \in k(x)[y]$ un polynôme de degré impair en y. Nous notons $\mathcal{C}$ la courbe hyperelliptique sur $k(x)$ d'équation affine*

$$\mathcal{C} : z^2 = f(x^2, y).$$

À tout $\delta \in k(x)^\times$ nous associons la $k(x)$-courbe hyperelliptique $\mathcal{C}_\delta$ d'équation affine

$$\mathcal{C}_\delta : t^2 = \delta^{\deg(f)} f\left(x, \frac{s}{\delta}\right).$$

Alors le $k(x)$-rang de Mordell-Weil de $Jac(\mathcal{C})$ est la somme des rangs de Mordell-Weil de $Jac(\mathcal{C}_1)(k(x))$ et $Jac(\mathcal{C}_x)(k(x))$.

Démonstration.

Le polynôme f est de degré impair en y. Les courbes $\mathcal{C}$ et $\mathcal{C}_\delta$ ont donc un point $k(x)$-rationnel au dessus du point à l'infini de $\mathbb{P}^1$, et donc $\mathrm{Jac}(\mathcal{C})(k(x))$ est isomorphe à $\mathrm{Pic}^0(k(x)(\mathcal{C}))$, et $\mathrm{Jac}(\mathcal{C}_\delta)(k(x))$ est isomorphe à $\mathrm{Pic}^0(k(x)(\mathcal{C}_\delta))$.

Nous notons ι : $\begin{array}{ccc} k(x)(\mathcal{C}) & \longrightarrow & k(x)(\mathcal{C}) \\ A(x,y,z) & \longmapsto & A(x,y,-z) \end{array}$ l'involution hyperelliptique et ρ l'involution de $k(x)(\mathcal{C})$ induite par l'automorphisme de $k(x)$ qui envoie x sur $-x$.

le morphisme ϕ_1 : $\begin{array}{ccc} k(x)(\mathcal{C}_1) & \longrightarrow & k(x)(\mathcal{C}) \\ A(x,s,t) & \longmapsto & A\left(x^2,y,z\right) \end{array}$ définit un isomorphisme de $k(x)(\mathcal{C}_1)$ dans $k(x^2)(\mathcal{C})$. Le corps $\mathrm{Im}(\phi_1)$ est un sous corps d'indice 2 de $k(x)(\mathcal{C})$. Or $k(x^2)(\mathcal{C}) \subset k(x)(\mathcal{C})^\rho$, donc $\mathrm{Im}(\phi_1)$ est égal à $k(x)(\mathcal{C})^\rho$.

De même, le morphisme ϕ_x : $\begin{array}{ccc} k(x)(\mathcal{C}_x) & \longrightarrow & k(x)(\mathcal{C}) \\ A(x,s,t) & \longmapsto & A(x^2, x^2y, x^{2\deg(f)+1}z) \end{array}$
est à valeur dans $k(x)(\mathcal{C})^{\iota\circ\rho}$. Or l'image de ϕ_x est un sous-corps d'indice 2 de $k(x)(\mathcal{C})$ (une base de $k(x)(\mathcal{C})$ en tant qu'espace vectoriel sur l'image de ϕ_x est $(1,x)$), donc $\mathrm{Im}(\phi_x)$ est égal à $k(x)(\mathcal{C})^{\iota\circ\rho}$.

Nous utilisons la proposition 3.2.6 : il existe un morphisme de groupe

$$\Psi : \mathrm{Jac}(\mathcal{C}_1)(k(x)) \times \mathrm{Jac}(\mathcal{C}_x)(k(x)) \longrightarrow \mathrm{Jac}(\mathcal{C})(k(x))$$

dont le noyau est fini et dont l'image contient $2\mathrm{Jac}(\mathcal{C})(k(x))$. Puisque $2\mathrm{Jac}(\mathcal{C})(k(x)) \subset \mathrm{Im}(\Psi)$, le rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})(k(x))$ est inférieur ou égal à la somme des rangs de Mordell-Weil de $\mathrm{Jac}(\mathcal{C}_1)(k(x))$ et $\mathrm{Jac}(\mathcal{C}_x)(k(x))$. Or le noyau de Ψ est fini, donc la somme des rangs de Mordell-Weil de $\mathrm{Jac}(\mathcal{C}_1)(k(x))$ et $\mathrm{Jac}(\mathcal{C}_x)(k(x))$ est inférieure ou égale au rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})(k(x))$. □

Proposition 3.2.10 *Soient B, $C \in \mathbb{R}(x)$ deux fractions rationnelles. Soit $\mathcal{C}$ la courbe hyperelliptique sur $\mathbb{R}(x)$ d'équation affine*

$$z^2 + (y^2+1)(y^2+C(x^2))(y^4 + (1+C(x^2))y^2 + B(x^2)) = 0.$$

Nous supposons que $B(x^2)$, $C(x^2)$, $B(x^2)C(x^2)$, $B(x^2) - C(x^2)$, $(B(x^2)-C(x^2))(1-C(x^2))$ et $(1+C(x^2))^2 - 4B(x^2)$ ne sont pas des carrés dans $\mathbb{C}(x)$.

À tout $\delta \in \mathbb{R}(x)^\times$ nous associons les $\mathbb{R}(x)$-courbes hyperelliptiques $\mathcal{C}_\delta^+$ et $\mathcal{C}_\delta^-$ d'équations affines respectives :

$\mathcal{C}_\delta^+ : z^2 = y(y-\delta)(y-\delta C(x))(y^2 - \delta[1+C(x)]y + \delta^2 B(x^2))$ *et*
$\mathcal{C}_\delta^- : t^2 = s(s^2 - \delta[(1-C(x^2))^2 - 2(B(x^2)-C(x^2))]s + \delta^2(B(x^2)-C(x^2))^2).$

Alors le $\mathbb{R}(x)$-rang de Mordell-Weil de $Jac(\mathcal{C})$ est la somme des rangs de Mordell-Weil de $Jac(\mathcal{C}_1^+)(\mathbb{R}(x))$, $Jac(\mathcal{C}_x^+)(\mathbb{R}(x))$, $Jac(\mathcal{C}_1^-)(\mathbb{R}(x))$ et $Jac(\mathcal{C}_x^-)(\mathbb{R}(x))$.

Démonstration.

Nous notons $\mathcal{C}^+$ et $\mathcal{C}^-$ les courbes hyperelliptiques sur $\mathbb{R}(x)$ d'équations affines respectives :

$\mathcal{C}^+ : t^2 = y(y-1)(y-C(x^2))(y^2 - [1+C(x^2)]y + B(x^2))$ et
$\mathcal{C}^- : t^2 = s(s^2 - [(1-C(x^2))^2 - 2(B(x^2)-C(x^2))]s + (B(x^2)-C(x^2))^2).$

D'après le corollaire 3.2.8, le $\mathbb{R}(x)$-rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})$ est la somme des $\mathbb{R}(x)$-rangs de Mordell-Weil de $\mathrm{Jac}(\mathcal{C}^+)$ et $\mathrm{Jac}(\mathcal{C}^-)$.

Il suffit maintenant d'appliquer la proposition 3.2.9 aux courbes hyperelliptiques $\mathcal{C}^+$ et $\mathcal{C}^-$:

* le $\mathbb{R}(x)$-rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C}^+)$ est la somme des $\mathbb{R}(x)$-rangs de Mordell-Weil de $\mathrm{Jac}(\mathcal{C}_1^+)$ et $\mathrm{Jac}(\mathcal{C}_x^+)$, et
* le $\mathbb{R}(x)$-rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C}^-)$ est la somme des $\mathbb{R}(x)$-rangs de Mordell-Weil de $\mathrm{Jac}(\mathcal{C}_1^-)$ et $\mathrm{Jac}(\mathcal{C}_x^-)$. □

3.3 Des conditions générales de descente

3.3.1 Une première étude de l'image des morphismes de Cassels-Schaefer

Notations 3.3.1.1 Soit k un corps de caractéristique 0. Si $P(y) \in k(x)[y]$ est un polynôme irréductible unitaire, nous posons $K_P := k(x)[y]/(P(y))$ et nous notons y_P la classe de y dans le quotient K_P.

Notations 3.3.1.2 Soit $h \in k[x][y]$ un polynôme unitaire de degré impair sans facteur carré. Nous considérons la courbe hyperelliptique $\mathcal{C}$ sur $k(x)$ d'équation affine

$$\mathcal{C} : z^2 = h(y).$$

Soit $h(y) = \prod_{l \in J} \mu_l(y)$ la décomposition en facteurs premiers de $h(y)$ (les facteurs μ_l sont choisis unitaires). Nous supposons que μ_l est un élément de $k[x][y]$ pour tout $l \in J$.

Soit $h'(y)$ la dérivée du polynôme $h(y)$ au sens usuel. Pour tout $l \in J$, nous désignons par T_l la classe $h'(y_{\mu_l})$ de $h'(y)$ dans $K_{\mu_l} = k(x)[y]/(\mu_l(y))$.

Dans la section 3.3.1, nous montrons la proposition 3.3.1.3 ci-dessous et sa conséquence la proposition 3.3.1.9.

Proposition 3.3.1.3 *Nous conservons les notations 3.3.1.1 et 3.3.1.2. Soit $l \in J$. Soit $div(u, v) \in Div(\mathcal{C})(k(x))$ un diviseur semi-réduit tel que u soit premier avec μ_l.*

Alors les places finies de K_{μ_l} en lesquelles la valuation de $u(y_{\mu_l})$ est impaire appartiennent au support de $div(T_l)$.

Notations 3.3.1.4 Soit $\mathrm{div}(u, v) \in \mathrm{Div}(\mathcal{C})(k(x))$ un diviseur semi-réduit tel que u soit premier avec h.

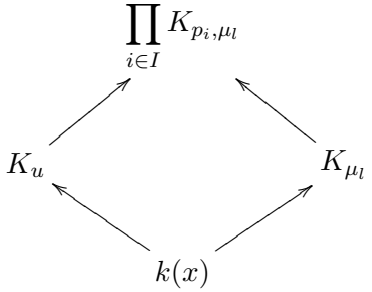
Nous fixons un indice $l \in J$. Soit $u(y) = \prod_{i \in I} p_i^{n_i}$ la décomposition de $u(y)$ en facteurs premiers dans $K_{\mu_l}[y]$. Nous pouvons choisir les p_i unitaires car u est lui même unitaire.

Nous fixons un indice $i \in I$. Nous notons $K_{p_i,\mu_l} := K_{\mu_l}[y]/(p_i(y))$, et nous désignons par $y_{p_i} \in K_{p_i,\mu_l}$ la classe de y modulo $p_i(y)$.

Soit $\mathfrak{p}$ une place finie de K_{μ_l} tel que $v_{\mathfrak{p}}(p_i(y_{\mu_l})) \neq 0$. Si $\mathcal{P}$ est une place de K_{p_i,μ_l} au dessus de la place $\mathfrak{p}$, nous désignons par $e(\mathcal{P}|\mathfrak{p})$ l'indice de ramification de $\mathcal{P}$ au dessus de $\mathfrak{p}$ et par $f(\mathcal{P}|\mathfrak{p})$ le degré relatif de $\mathcal{P}$ au dessus de $\mathfrak{p}$.

Pour démontrer la proposition 3.3.1.3, nous allons étudier la parité des valuations des éléments $p_i(y_{\mu_l}) \in K_{\mu_l}$ en les places de K_{μ_l}. Nous cherchons pour cela à tirer profit de la définition de la représentation de Mumford et

en particulier de la congruence $h(y) \equiv (v(y))^2 \bmod u(y)$. Malheureusement cette congruence correspond à une égalité dans l'algèbre $K_u := k(x)[y]/(u(y))$, alors que nous souhaitons une information sur la classe $p_i(y_{\mu_l}) \in K_{\mu_l}$. Cela motive l'introduction des corps de fonctions K_{p_i,μ_l} : nous disposons d'un diagramme commutatif



L'idée est alors de calculer la parité de $v_{\mathfrak{p}}(p_i(y_{\mu_l}))$ à l'aide de valuations en les places du corps de fonctions K_{p_i,μ_l}.

La proposition suivante est classique dans le cadre des anneaux de Dedekind. Faute de référence dans le cadre des corps de fonctions, nous avons choisi de la redémontrer.

Proposition 3.3.1.5 *Soient k un corps et F un corps de fonctions sur k. Soit $\widetilde{F}$ une extension finie du corps F. Soit $\mathfrak{p}$ une place du corps de fonctions F. Si $\mathcal{P}$ est une place au dessus de $\mathfrak{p}$, nous notons $f(\mathcal{P}|\mathfrak{p})$ le degré relatif de $\mathcal{P}$ au dessus de $\mathfrak{p}$. Soit $R \in \widetilde{F}$.*

Alors la valuation $v_{\mathfrak{p}}(N_{\widetilde{F}/F}(R))$ est égale à $\displaystyle\sum_{\mathcal{P} \text{ place de } \widetilde{F}, \mathcal{P}|\mathfrak{p}} f(\mathcal{P}|\mathfrak{p}) v_{\mathcal{P}}(R)$.

Démonstration.

Soit F_2 une clôture galoisienne L' de l'extension $\widetilde{F}/F$. Nous posons $G := \mathrm{Gal}(F_2/F)$. Nous calculons la valuation $v_{\mathfrak{p}}(N_{F_2/F}(R))$ de deux façons différentes.

Soit $\mathfrak{P}_0$ une place de F_2 au dessus de $\mathfrak{p}$. L'extension F_2/F est galoisienne, donc $N_{F_2/F}(R) = \prod_{\sigma\in G} \sigma(R)$, et donc

$$v_{\mathfrak{P}_0}(N_{F_2/F}(R) = \sum_{\sigma\in G} v_{\mathfrak{P}_0}(\sigma(R)) = \sum_{\sigma\in G} v_{\sigma^{-1}(\mathfrak{P}_0)}(R).$$

D'après [Sti93] Théorème III.7.2, l'indice de ramification $e(\mathfrak{P}_0|\mathfrak{p})$ et le degré relatif $f(\mathfrak{P}_0|\mathfrak{p})$ ne dépendent pas du choix de la place $\mathfrak{P}_0$ au dessus de $\mathfrak{p}$. Nous notons $e(\mathfrak{p}) := e(\mathfrak{P}_0|\mathfrak{p})$ et $f(\mathfrak{p}) := f(\mathfrak{P}_0|\mathfrak{p})$.

Nous déterminons l'orbite de $\mathfrak{P}_0$ sous G en utilisant [Sti93] Théorème III.7.1 : cette orbite est l'ensemble des places de F_2 au dessus de $\mathfrak{p}$. Pour

calculer la somme $\sum_{\sigma\in G} v_{\sigma^{-1}(\mathfrak{P}_0)}(R)$ nous remarquons que, pour toute place $\mathfrak{P}$ de F_2 au dessus de $\mathfrak{p}$, le cardinal du groupe de décomposition de $\mathfrak{P}$ au dessus de $\mathfrak{p}$ est $e(\mathfrak{p})f(\mathfrak{p})$ (voir [Sti93] Théorème III.8.2). Ainsi la valuation $v_{\mathfrak{P}_0}(N_{F_2/F}(R))$ est égale à $\sum_{\mathfrak{P} \text{ place de } F_2, \mathfrak{P}|\mathfrak{p}} e(\mathfrak{p})f(\mathfrak{p})v_{\mathfrak{P}}(R)$. Or $v_{\mathfrak{P}_0}(N_{F_2/F}(R)) = e(\mathfrak{p})v_{\mathfrak{p}}(N_{F_2/F}(R))$, donc la valuation $v_{\mathfrak{p}}(N_{F_2/F}(R))$ est égale à $\sum_{\mathfrak{P} \text{ place de } F_2, \mathfrak{P}|\mathfrak{p}} f(\mathfrak{p})v_{\mathfrak{P}}(R) = \sum_{\mathfrak{P} \text{ place de } F_2, \mathfrak{P}|\mathfrak{p}} f(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{P}}(R)$.

Pour conclure nous utilisons les égalités suivantes :

* $v_{\mathfrak{p}}(N_{F_2/F}(R)) = v_{\mathfrak{p}}(N_{F_2/\widetilde{F}}(N_{\widetilde{F}/F}(R))) = [F_2 : \widetilde{F}]v_{\mathfrak{p}}(N_{\widetilde{F}/F}(R))$,
* pour toute place $\mathcal{P}$ de $\widetilde{F}$ au dessus $\mathfrak{p}$ et toute place $\mathfrak{P}$ de F_2 au dessus de $\mathcal{P}$, nous avons $f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathcal{P})f(\mathcal{P}|\mathfrak{p})$ (voir [Sti93] Théorème III.1.6) et $v_{\mathfrak{P}}(R) = e(\mathfrak{P}|\mathcal{P})v_{\mathcal{P}}(R)$, et
* pour toute place $\mathcal{P}$ de $\widetilde{F}$ au dessus $\mathfrak{p}$, nous avons

$$[F_2 : \widetilde{F}] = \sum_{\mathfrak{P} \text{ place de } F_2, \mathfrak{P}|\mathcal{P}} f(\mathfrak{P}|\mathcal{P})e(\mathfrak{P}|\mathcal{P})$$

(voir [Sti93] Théorème III.1.6).

Nous en déduisons en effet que

$$\begin{aligned}
[F_2 : \widetilde{F}]v_{\mathfrak{p}}(N_{\widetilde{F}/F}(R)) &= \sum_{\mathfrak{P} \text{ place de } F_2, \mathfrak{P}|\mathfrak{p}} f(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{P}}(R) \\
&= \sum_{\mathcal{P} \text{ place de } \widetilde{F}, \mathcal{P}|\mathfrak{p}} \left(\sum_{\mathfrak{P} \text{ place de } F_2, \mathfrak{P}|\mathcal{P}} f(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{P}}(R) \right) \\
&= \sum_{\mathcal{P} \text{ place de } \widetilde{F}, \mathcal{P}|\mathfrak{p}} \left(\sum_{\mathfrak{P} \text{ place de } F_2, \mathfrak{P}|\mathcal{P}} f(\mathfrak{P}|\mathcal{P})f(\mathcal{P}|\mathfrak{p})e(\mathfrak{P}|\mathcal{P})v_{\mathcal{P}}(R) \right) \\
&= \sum_{\mathcal{P} \text{ place de } \widetilde{F}, \mathcal{P}|\mathfrak{p}} \left(\sum_{\mathfrak{P} \text{ place de } F_2, \mathfrak{P}|\mathcal{P}} f(\mathfrak{P}|\mathcal{P})e(\mathfrak{P}|\mathcal{P}) \right) f(\mathcal{P}|\mathfrak{p})v_{\mathcal{P}}(R) \\
&= \sum_{\mathcal{P} \text{ place de } \widetilde{F}, \mathcal{P}|\mathfrak{p}} [F_2 : \widetilde{F}]f(\mathcal{P}|\mathfrak{p})v_{\mathcal{P}}(R) \quad \square
\end{aligned}$$

Lemme 3.3.1.6 *Nous conservons les notations 3.3.1.1, 3.3.1.2 et 3.3.1.4. Soit $\alpha \in K_{\mu_l}$ un élément non nul. Nous supposons que la valuation $v_{\mathfrak{p}}(\alpha)$ est positive ou nulle.*

Alors, pour toute place $\mathcal{P}$ de K_{p_i,μ_l} au dessus de $\mathfrak{p}$, la valuation $v_{\mathcal{P}}(\alpha)$ est positive ou nulle.

Démonstration.

Soit $\mathcal{P}$ une place de K_{p_i,μ_l} au dessus de $\mathfrak{p}$. La valuation $v_{\mathfrak{p}}(\alpha)$ est positive ou nulle. Or l'indice de ramification $e(\mathcal{P}|\mathfrak{p})$ est positif, donc la valuation $v_{\mathcal{P}}(\alpha) = e(\mathcal{P}|\mathfrak{p})v_{\mathfrak{p}}(\alpha)$ est positive ou nulle. □

Lemme 3.3.1.7 *Nous conservons les notations 3.3.1.1, 3.3.1.2 et 3.3.1.4. Soit $\mathcal{P}$ une place de K_{p_i,μ_l} au dessus de $\mathfrak{p}$ telle que $v_{\mathcal{P}}(T_l) = 0$. Nous notons h_j le coefficient devant $(y-y_{\mu_l})^{j+1}$ dans le polynôme $h(y) = h((y-y_{\mu_l})+y_{\mu_l})$. Nous supposons que $v_{\mathcal{P}}(y_{p_i} - y_{\mu_l}) \neq 0$.*

Alors la valuation $v_{\mathcal{P}}\left(T_l + (y_{p_i} - y_{\mu_l})^{2g} + \sum_{j=1}^{2g-1} h_j(y_{p_i} - y_{\mu_l})^j\right)$ *est paire.*

Démonstration.

L'élément y_{μ_l} est une racine dans K_{μ_l} du polynôme μ_l. Or $\mu_l(y) \in k[x][y]$, donc y_{μ_l} est un élément de la fermeture intégrale de $k[x]$ dans K_{μ_l}. En particulier la valuation $v_{\mathfrak{p}}(y_{\mu_l})$ est positive ou nulle (voir [Sti93] Théorème III.2.6).

Soit $p \in k[x]$ l'unique polynôme irréductible unitaire tel que $\mathfrak{p}$ soit une place au dessus de p. Comme $h(y) \in k[x][y]$, les coefficients de $h(y)$ sont soit nuls soit de valuation positive ou nulle en p. Puisque l'indice de ramification $e(\mathfrak{p}|p)$ de $\mathfrak{p}$ au dessus de p est positif, les coefficients de $h(y)$ sont soit nuls soit de valuation positive ou nulle en $\mathfrak{p}$.

Les coefficients h_j sont des polynômes en y_{μ_l} et les coefficients de $h(y)$. Par conséquent les coefficients h_j sont soit nuls soit de valuation positive ou nulle en $\mathfrak{p}$. Ainsi, d'après le lemme 3.3.1.6, les coefficients h_j sont soit nuls soit de valuation positive ou nulle en $\mathcal{P}$.

Nous supposons tout d'abord que $v_{\mathcal{P}}(y_{p_i} - y_{\mu_l}) > 0$. Soit $j \in \{1, \cdots, 2g\}$. La valuation $v_{\mathcal{P}}((y_{p_i} - y_{\mu_l})^j) = jv_{\mathcal{P}}((y_{p_i} - y_{\mu_l}))$ est strictement positive. En particulier nous savons que $h_j(y_{p_i} - y_{\mu_l})^j = 0$ ou $v_{\mathcal{P}}(h_j(y_{p_i} - y_{\mu_l})^j) > 0$. Or la valuation $v_{\mathcal{P}}(T_l)$ est nulle, donc, par inégalité triangulaire, nous avons

$$v_{\mathcal{P}}\left(T_l + (y_{p_i} - y_{\mu_l})^{2g} + \sum_{j=1}^{2g-1} h_j(y_{p_i} - y_{\mu_l})^j\right) = v_{\mathcal{P}}(T_l) = 0.$$

Nous supposons maintenant que $v_{\mathcal{P}}(y_{p_i} - y_{\mu_l}) < 0$. Soit $j \in \{1, \cdots, 2g\}$. La valuation $v_{\mathcal{P}}((y_{p_i} - y_{\mu_l})^j) = jv_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$ est strictement supérieure à $2gv_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$. Ainsi, nous savons que $h_j(y_{p_i} - y_{\mu_l})^j = 0$ ou $v_{\mathcal{P}}(h_j(y_{p_i} - y_{\mu_l})^j) > 2gv_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$. Nous montrons donc, par inégalité triangulaire, que la valuation $v_{\mathcal{P}}\left(\sum_{j=1}^{2g-1} h_j(y_{p_i} - y_{\mu_l})^j\right)$ est strictement supérieure à $2gv_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$. De plus, la valuation $v_{\mathcal{P}}(T_l)$ est nulle et donc strictement

supérieure à $2gv_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$. En appliquant l'inégalité triangulaire, nous obtenons finalement

$$v_{\mathcal{P}}\left(T_l + (y_{p_i} - y_{\mu_l})^{2g} + \sum_{j=1}^{2g-1} h_j (y_{p_i} - y_{\mu_l})^j\right) = 2gv_{\mathcal{P}}(y_{p_i} - y_{\mu_l}). \quad \square$$

Lemme 3.3.1.8 *Nous conservons les notations 3.3.1.1, 3.3.1.2 et 3.3.1.4. Soit $\mathcal{P}$ une place de K_{p_i,μ_l} au dessus de $\mathfrak{p}$ telle que $v_{\mathcal{P}}(T_l) = 0$. Nous notons h_j le coefficient devant $(y-y_{\mu_l})^{j+1}$ dans le polynôme $h(y) = h((y-y_{\mu_l})+y_{\mu_l})$.*

Alors la valuation $v_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$ est paire.

Démonstration.

Nous supposons que la valuation $v_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$ est non nulle (l'autre cas est direct). Par hypothèse (voir les notations 3.3.1.4), les polynômes p_i et h sont premiers entre eux. De la congruence $h(y) \equiv v(y)^2 \bmod p_i(y)$ nous déduisons que la valuation $v_{\mathcal{P}}(h(y_{p_i}))$ est paire.

Comme $\mu_l(y)$ divise $h(y)$, l'élément $h(y_{\mu_l})$ est nul, et donc

$$h(y) = (y - y_{\mu_l})\left(T_l + (y - y_{\mu_l})^{2g} + (\sum_{j=1}^{2g-1} h_j (y - y_{\mu_l})^j)\right) \tag{3.2}$$

(nous rappelons que $T_l = h'(y_{\mu_l})$ est la classe de $h'(y)$ modulo $\mu_l(y)$). Ainsi, en réduisant l'égalité 3.2 modulo $p_i(y)$ (c'est-à-dire en l'évaluant en y_{p_i}) et en utilisant la parité de $v_{\mathcal{P}}(h(y_{p_i}))$, nous montrons la congruence

$$v_{\mathcal{P}}(y_{p_i} - y_{\mu_l}) \equiv v_{\mathcal{P}}\left(T_l + (y_{p_i} - y_{\mu_l})^{2g} + (\sum_{j=1}^{2g-1} h_j (y_{p_i} - y_{\mu_l})^j)\right) \bmod 2.$$

Pour conclure il suffit d'appliquer le lemme 3.3.1.7. $\square$

Démonstration de la proposition 3.3.1.3.

Nous reprenons les notations 3.3.1.4. Supposons par l'absurde que la valuation de T_l en $\mathfrak{p}$ soit nulle. Alors, toutes les valuations $v_{\mathcal{P}}(T_l) = e(\mathcal{P}|\mathfrak{p})v_{\mathfrak{p}}(T_l)$ sont nulles, et ainsi, les hypothèses du lemme 3.3.1.8 sont vérifiées. Par conséquent, toutes les valuations $v_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$ sont paires. Nous faisons appel à la proposition 3.3.1.5 : comme $p_i(y_{\mu_l}) = N_{K_{p_i,\mu_l}/K_{\mu_l}}(y_{p_i} - y_{\mu_l})$, la valuation $v_{\mathfrak{p}}(p_i(y_{\mu_l}))$ est paire. Ceci est en contradiction avec le choix de $\mathfrak{p}$. $\square$

Nous présentons maintenant une première application de la proposition 3.3.1.3. Cette application nous permet, lors de la sous-section 3.3.2, d'effectuer une 2-descente. La proposition 3.3.1.3 est également utilisée au cours de la section 4.1 pour montrer que certains rangs de Mordell-Weil sont nuls.

Proposition 3.3.1.9 *Soit k un sous-corps de $\mathbb{R}$. Soient $h(y) \in k[x][y]$ un polynôme unitaire, de degré impair $2g+1$, sans facteur carré, et $\mathcal{C}$ la courbe hyperelliptique définie sur $k(x)$ par l'équation affine $z^2 = h(y)$. Nous supposons qu'il existe $2g$ éléments $e_1, \cdots, e_{2g-1}$, $H \in k[x]$ et un polynôme $\mu(y) \in k[x][y]$ de degré 2 tels que $h(y) = \mu(y) \prod_{i=1}^{2g-1} (y - He_i)$. Nous supposons de plus que :*

* *le discriminant $\Delta(h)$ de $h(y)$ est scindé sur k,*
* *le discriminant $\Delta(\mu)$ de μ est de la forme H^2Q^2D avec $D \in k[x]$ un polynôme de degré 1 et $Q \in k[x]$,*
* *$\Delta(h) = Q^2Q_1$ avec $Q_1 \in k[x]$ premier à Q, et*
* *pour toute racine $\alpha \in k$ de H, l'élément $D(\alpha)$ est un carré dans k.*

Soient $L := \mathbb{C}(x)[t]/(h(t))$ et $\pi_{\mathcal{C}} : Jac(\mathcal{C})(\mathbb{C}(x)) \longrightarrow L^\times/L^{\times 2}$ le morphisme de Cassels-Schaefer associé à $Jac(\mathcal{C})(\mathbb{C}(x))$.

Alors l'image de $\pi_{\mathcal{C}}$ est laissée invariante par l'action de $Gal(\mathbb{C}/k)$.

Lemme 3.3.1.10 *Nous conservons les notations et hypothèses de la proposition 3.3.1.9. Nous supposons de plus que le polynôme μ est irréductible. Nous notons $K_{\mu,\mathbb{C}} := \mathbb{C}(x)[y]/(\mu(y))$ et nous désignons par y_μ la classe de y dans le quotient $K_{\mu,\mathbb{C}}$. Soit $s := \frac{\mu'(y_\mu)}{2HQ}$.*

Alors le polynôme minimal de s sur $\mathbb{C}(x)$ est $y^2 - D(x)$. Par suite, l'anneau $\mathbb{C}[x,s]$ est factoriel et son corps de fraction est $K_{\mu,\mathbb{C}}$.

Démonstration.

La dérivée $\mu'(y)$ est un polynôme de degré 1 en y et de coefficient dominant 2. Ainsi, le corps $\mathbb{C}(x,s)$ contient x et y_μ. Le corps des fractions de $\mathbb{C}[x,s]$ est donc bien $K_{\mu,\mathbb{C}}$.

Par ailleurs, le discriminant du polynôme $\mu(T)$ est H^2Q^2D. Il existe donc $\alpha \in k$ tel que $\mu(T) = (T+\alpha)^2 - H^2Q^2D$. Nous avons alors $2(T+\alpha) = \mu'(T)$, c'est-à-dire que $\mu(T) = \left(\frac{\mu'(T)}{2}\right)^2 - H^2Q^2D$. Par suite, $s^2 - D = \frac{\mu(y_\mu)}{H^2Q^2} = 0$: le polynôme minimal de s divise $T^2 - D$. Or $s \notin \mathbb{C}(x)$, donc le polynôme minimal de s est $T^2 - D$.

Enfin, l'anneau $\mathbb{C}[x,s]$ est factoriel car $\mathbb{C}[x,s] = \mathbb{C}[D,s] = \mathbb{C}[s]$ (le polynôme $D \in k[x]$ est de degré 1). $\square$

Lemme 3.3.1.11 *Nous conservons les notations et hypothèses du lemme 3.3.1.10. Soient $\alpha \in k$ une racine du résultant $Res_T(h'(T), \mu(T))$ telle que $Q(\alpha) \neq 0$ et β un élément premier de $\mathbb{C}[x,s]$ tel que $N_{K_{\mu,\mathbb{C}}/\mathbb{C}(x)}(\beta) = \lambda(x-\alpha)$ pour un certain $\lambda \in \mathbb{C}$.*

Alors la valuation v_β est invariante sous $Gal(\mathbb{C}/k)$. En particulier, pour tout diviseur semi-réduit $div(u,v) \in Div^0(\mathbb{C}(x)(\mathcal{C}))$, et tout $\sigma \in Gal(\mathbb{C}/k)$, la valuation $v_\beta(u(y_\mu)\sigma(u(y_\mu)))$ est paire.

Démonstration.

Puisque $\beta \in \mathbb{C}[x,s]$, il existe β_0, $\beta_1 \in \mathbb{C}[x]$ tels que $\beta = \beta_1 s + \beta_0$. Le polynôme minimal de s sur $\mathbb{C}(x)$ est $T^2 - D(x)$. Nous avons donc

$$\lambda(x-\alpha) = N_{\mathbb{C}(x)(s)/\mathbb{C}(x)}(\beta) = \beta_0^2 - \beta_1^2 D. \tag{3.3}$$

Or le polynôme D est de degré 1, donc β_1 et β_0 sont des éléments de $\mathbb{C}$, et β_1 est non nul. De plus, en évaluant l'égalité 3.3 en α, nous obtenons $\beta_0^2 = \beta_1^2 D(\alpha)$.

L'élément $\alpha \in k$ est une racine du résultant

$$\begin{aligned} \mathrm{Res}_T(h'(T),\mu(T)) &= \mathrm{Res}_T(\mu'(T),\mu(T)) \prod_{i=1}^{2g-1} \mathrm{Res}_T(T - He_i, \mu(T)) \\ &= \Delta(\mu) \prod_{i=1}^{2g-1} \mu(He_i), \end{aligned}$$

L'élément $\alpha \in k$ est donc soit une racine du discriminant $\Delta(\mu) = H^2Q^2D$ de μ soit une racine de $\mu(He_i)$ pour un certain entier $i \in \{1, \cdots 2g-1\}$.

Lorsque α est racine de $\mu(He_i)$ pour un entier $i \in \{1, \cdots 2g-1\}$, mais n'est pas racine de H. Nous écrivons la formule de Taylor pour $\mu(T)$ en He_i

$$\mu(T) = (T - He_i)^2 + (T - He_i)\mu'(He_i) + \mu(He_i).$$

Le discriminant $\Delta(\mu)$ est donc égal à $(\mu'(He_i))^2 - 4\mu(H_{e_i})$. Comme α est une racine de $\mu(He_i)$, nous avons

$$\begin{aligned} H(\alpha)^2 Q(\alpha)^2 D(\alpha) = \Delta(\mu)(\alpha) &= (\mu'(He_i)(\alpha))^2 - 4\mu(H_{e_i})(\alpha) \\ &= (\mu'(He_i)(\alpha))^2 . \end{aligned}$$

Or α n'est pas une racine de HQ, donc $D(\alpha)$ est un carré dans k. Ainsi, puisque $\beta_0^2 = \beta_1^2 D$, le quotient $\frac{\beta_0}{\beta_1}$ appartient à k.

Lorsque α est une racine de D. Alors $\frac{\beta_0}{\beta_1} = 0$ appartient à k.

Lorsque α est un racine de H. Dans l'énoncé de la proposition 3.3.1.9, nous avons supposé que $D(\alpha)$ est un carré dans k. Ainsi, puisque $\beta_0^2 = \beta_1^2 D$, le quotient $\frac{\beta_0}{\beta_1}$ appartient à k.

Nous posons $\Lambda := \beta_1$. Nous venons de montrer que $\Lambda^{-2}\beta = \left(s - \frac{\beta_0}{\beta_1}\right)$ est un élément de $k(x)[s] = k(x)[y_\mu]$ (car $s = \frac{\mu'(y_\mu)}{2HQ} \in k(x)[y_\mu]$). Nous en déduisons que la valuation v_β est invariante sous $\mathrm{Gal}(\mathbb{C}/k)$. En particulier, pour tout $\sigma \in \mathrm{Gal}(\mathbb{C}/k)$, nous avons

$$\begin{aligned} v_\beta(u(y_\mu)\sigma(u(y_\mu))) &= v_\beta(u(y_\mu)) + v_\beta(\sigma(u(y_\mu))) \\ &= v_\beta(u(y_\mu)) + v_{\sigma^{-1}(\beta)}(u(y_\mu)) \\ &= 2v_\beta(u(y_\mu)) \\ &\equiv 0 \bmod 2. \quad \square \end{aligned}$$

Lemme 3.3.1.12 *Nous conservons les notations et hypothèses du lemme 3.3.1.10. Soient $\alpha \in k$ une racine de Q et β un élément premier de $\mathbb{C}[x,s]$ tel que $N_{K_{\mu,\mathbb{C}}/\mathbb{C}(x)}(\beta) = \lambda(x-\alpha)$ pour un certain $\lambda \in \mathbb{C}$.*

Alors, pour tout diviseur semi-réduit $div(u,v) \in Div^0(\mathbb{C}(x)(\mathcal{C}))$, et tout $\sigma \in Gal(\mathbb{C}/k)$, la valuation $v_\beta(u(y_\mu)\sigma(u(y_\mu)))$ est paire.

Démonstration.

Soit $\sigma \in \mathrm{Gal}(\mathbb{C}/k)$. Nous appliquons la formule de Taylor à $\mu(T)$ en y_μ

$$\begin{aligned}\mu(T) &= \mu(y_\mu) + \mu'(y_\mu)(T-y_\mu) + (T-y_\mu)^2 \\ &= (T-y_\mu)(\mu'(y_\mu) + (T-y_\mu)).\end{aligned}$$

Le polynôme $\mu(T)$ est donc scindé sur $K_{\mu,\mathbb{C}}$ et ses deux racines sont y_μ et $y_\mu - \mu'(y_\mu)$. Ainsi, il existe un unique $\mathbb{C}(x)$-automorphisme ι de $K_{\mu,\mathbb{C}}$ tel que $\iota(y_\mu) = y_\mu - \mu'(y_\mu)$. De plus, pour tout élément $\nu \in K_{\mu,\mathbb{C}}$, nous avons $N_{K_{\mu,\mathbb{C}}/\mathbb{C}(x)}(\nu) = \nu\iota(\nu)$.

Lorsque les valuations v_β et $v_{\sigma^{-1}(\beta)}$ sont égales, le résultat est direct. Nous supposons donc que les valuations v_β et $v_{\sigma^{-1}(\beta)}$ sont différentes.

L'élément β est premier. Les éléments $\iota(\beta)$ et $\sigma^{-1}(\beta)$ sont donc aussi premiers. Dans l'anneau factoriel $\mathbb{C}[x,s]$, la décomposition en facteurs premiers de $x-\alpha$ est donc donnée par l'égalité $\beta\iota(\beta) = N_{K_{\mu,\mathbb{C}}/\mathbb{C}(x)}(\beta) = \lambda(x-\alpha)$. Or $\sigma^{-1}(x-\alpha) = x-\alpha$ donc la décomposition en facteurs premiers de $x-\alpha$ dans $\mathbb{C}[x,s]$ est également donnée par $\sigma^{-1}(\beta)\sigma^{-1}(\iota(\beta)) = \sigma^{-1}(\lambda)(x-\alpha)$. Par unicité de la décomposition en facteurs premiers, il existe donc $\varepsilon \in \mathbb{C}^\times$ tel que $\sigma^{-1}(\beta) = \varepsilon\beta$ ou $\sigma^{-1}(\beta) = \varepsilon\iota(\beta)$. En particulier la valuation $v_{\sigma^{-1}(\beta)}$ est égale à v_β ou $v_{\iota(\beta)}$. Or les valuations v_β et $v_{\sigma^{-1}(\beta)}$ sont différentes, donc $v_{\sigma^{-1}(\beta)} = v_{\iota(\beta)}$.

Soit $p \in \mathbb{C}(x)[y]$ un facteur premier de $u(y)$ sur $\mathbb{C}(x)$. Nous notons $L_{p,\mu,\mathbb{C}} := K_{\mu,\mathbb{C}}[y]/(p(y))$ et nous désignons par y_p la classe de y dans le quotient $L_{p,\mu,\mathbb{C}}$.

Le couple (u,v) étant la représentation de Mumford d'un diviseur semi-réduit (un élément de $\mathrm{Div}^0(K_{\mu,\mathbb{C}}(\mathcal{C}))$), nous savons que $(v(y_p))^2 = h(y_p)$. Nous en déduisons que

$$\begin{aligned}(v(y_p))^2 &= \mu(y_p)\prod_{i=1}^{2g-1}(y_p - He_i) \\ &= (\mu(y_\mu) + \mu'(y_\mu)(y_p-y_\mu) + (y_p-y_\mu)^2)\prod_{i=1}^{2g-1}(y_p - He_i) \\ &= (y_p-y_\mu)(\mu'(y_\mu) + (y_p-y_\mu))\prod_{i=1}^{2g-1}(y_p - He_i)\end{aligned}$$

En appliquant la norme $N_{L_{p,\mu,\mathbb{C}}/K_{\mu,\mathbb{C}}}$ nous obtenons donc l'égalité

$$N_{L_{p,\mu,\mathbb{C}}/K_{\mu,\mathbb{C}}}(v(y_p))^2 = p(y_\mu)p(y_\mu - \mu'(y_\mu))\prod_{i=1}^{2g-1}p(He_i). \qquad (3.4)$$

D'après la proposition 3.3.1.3, si l'élément $p(He_i)$ à une valuation impaire en $x-\alpha$, alors $x-\alpha$ est un diviseur de $h'(He_i)$. Or $h'(He_i) = \mu(He_i)\prod_{j\neq i} H(e_i-e_j)$ est un diviseur de Q_1, et Q_1 et Q sont premiers entre eux, donc $h'(He_i)$ ne s'annule pas en α. La valuation de $p(He_i)$ en $x-\alpha$ est donc paire. Nous en déduisons que la valuation $v_\beta(p(He_i)) = e(\beta|x-\alpha)v_{x-\alpha}(p(He_i))$ est paire. Ainsi, l'équation 3.4 a pour conséquence que la valuation

$$\begin{aligned} v_\beta(p(y_\mu)p(y_\mu-\mu'(y_\mu))) &= v_\beta(p(y_\mu)\iota(p(y_\mu))) \\ &= v_\beta(p(y_\mu)) + v_\beta(\iota(p(y_\mu))) \\ &= v_\beta(p(y_\mu)) + v_{\iota(\beta)}(p(y_\mu)) \\ &= v_\beta(p(y_\mu)) + v_{\sigma^{-1}(\beta)}(p(y_\mu)) \\ &= v_\beta(p(y_\mu)) + v_\beta(\sigma(p(y_\mu))) \\ &= v_\beta(p(y_\mu)\sigma(p(y_\mu))) \end{aligned}$$

est paire. Ceci étant vrai pour tout facteur premier p de $u(T)$, nous concluons que la valuation $v_\beta(u(y_\mu)\sigma(u(y_\mu)))$ est paire. □

Démonstration de la proposition 3.3.1.9.

À tout facteur premier p de h, nous associons le corps $K_{p,\mathbb{C}} := \mathbb{C}(x)[y]/(p(y))$ et nous notons y_p la classe de y dans le quotient $K_{p,\mathbb{C}}$.

Soient $\alpha \in \mathrm{Im}(\pi_{\mathcal{C}})$ et $\mathrm{div}(u,v) \in \mathrm{Div}^0(\mathbb{C}(x)(\mathcal{C}))$ un diviseur semi-réduit tel que

* les polynômes u et h soient premiers entre eux, et
* la classe de $(-1)^{\deg(u)}u(t)$ dans $L^\times/L^{\times 2}$ soit un représentant de α.

Soit $\sigma \in \mathrm{Gal}(\mathbb{C}/k)$. Par définition de $\pi_{\mathcal{C}}$, la classe α est σ-invariante si et seulement si, pour tout facteur premier p de h, la classe $u(y_p)\sigma(u)(y_p)$ est un carré dans $K_{p,\mathbb{C}}$.

Soit p un facteur premier de h. Sous les hypothèses de la proposition, le corps de fonctions $K_{p,\mathbb{C}}$ est le corps de fraction d'un anneau factoriel $\mathcal{O}_{p,\mathbb{C}}$ (c.f. le lemme 3.3.1.10 pour le cas où $K_{p,\mathbb{C}} \neq k(x)$). Nous décomposons $u(y_p)$ en facteur premiers : $u(y_p) =: \varepsilon\prod_{i\in I}\beta_i^{n_i}$ avec $\varepsilon \in \mathcal{O}_{p,\mathbb{C}}^\times$ et β_i un élément premier de $\mathcal{O}_{p,\mathbb{C}}$. Soit $I' \subset I$ l'ensemble des indices i tels que n_i soit impaire. Tout élément de $\mathbb{C}$ étant un carré dans $\mathbb{C}$, nous avons équivalence entre

* $u(y_p)\sigma(u)(y_p) \in K_{p,\mathbb{C}}^{\times 2}$, et
* pour tout $i \in I'$, la valuation $v_{\beta_i}(u(y_p)\sigma(u(y_p)))$ est paire.

Soit $i \in I'$. Nous appliquons la proposition 3.3.1.3 : la valuation de $h'(y_p)$ en β_i est non nulle. La norme $N_{K_{p,\mathbb{C}}/\mathbb{C}(x)}(\beta_i)$ est donc un facteur premier de la norme $N_{K_{p,\mathbb{C}}/\mathbb{C}(x)}(h'(y_p)) = \mathrm{Res}_T(h'(T),p(T)) \in k[x]$. Or le résultant $\mathrm{Res}_T(h'(T),p(T))$ divise $\Delta(h)$ (car p est un facteur premier de h), donc la norme $N_{K_{p,\mathbb{C}}/\mathbb{C}(x)}(\beta_i)$ est un facteur premier de $\Delta(h)$. Le polynôme $\Delta(h)$

étant supposé scindé sur k, il existe $\lambda \in \mathbb{C}^\times$ et une racine $\alpha \in k$ du résultant $\mathrm{Res}_T(h'(T), p(T))$ tels que $N_{K_{p,\mathbb{C}}/\mathbb{C}(x)}(\beta_i) = \lambda(x-\alpha)$.

Si p est de degré 1 en y. Soit $\Lambda \in \mathbb{C}^\times$ tel que $\Lambda^2 = \lambda$. Nous avons alors $K_{p,\mathbb{C}} = \mathbb{C}(x)$ et donc $\beta_i = N_{K_{p,\mathbb{C}}/\mathbb{C}(x)}(\beta_i)$. Cette égalité se reformule sous la forme $\Lambda^{-2}\beta_i = \lambda\beta_i = (x-\alpha)$. Par suite, $\Lambda^{-2}\beta_i$ est un élément de $k(x)[y]/(p(y))$. En particulier, les valuations v_{β_i} et $v_{\sigma^{-1}(\beta_i)}$ sont égales. Nous en déduisons que la valuation

$$\begin{aligned} v_{\beta_i}(u(y_p)\sigma(u(y_p))) &= v_{\beta_i}(u(y_p)) + v_{\beta_i}(\sigma(u(y_p))) \\ &= v_{\beta_i}(u(y_p)) + v_{\sigma^{-1}(\beta_i)}(u(y_p)) \\ &= 2v_{\beta_i}(u(y_p)) \end{aligned}$$

est paire.

Si $p = \mu$ est un polynôme irréductible. Nous utilisons les lemmes 3.3.1.11 et 3.3.1.12 : pour tout $i \in I'$, la valuation $v_{\beta_i}(u(y_p)\sigma(u(y_p)))$ est paire. □

3.3.2 La 2-descente.

Nous considérons un polynôme $f \in \mathbb{R}(x)[y]$ sans facteur carré de degré impair et la courbe hyperelliptique $\mathcal{C}$ sur $\mathbb{R}(x)$ d'équation affine $z^2 = f(y)$. Nous souhaitons calculer le rang de Mordell-Weil de la jacobienne $J := \mathrm{Jac}(\mathcal{C})$ sur $\mathbb{R}(x)$. Plus exactement, nous voulons montrer que ce rang de Mordell-Weil est nul. Pour cela, nous commençons par effectuer une 2-descente.

Corollaire 3.3.2.1 *Soit k_0 un sous-corps de $\mathbb{C}$. Soient $f \in k_0(x)[y]$ un polynôme sans facteur carré de degré impair et $\mathcal{C}$ la courbe hyperelliptique sur $k_0(x)$ d'équation affine $z^2 = f(y)$. Soit J la jacobienne de $\mathcal{C}$. Nous supposons que la torsion 2-primaire de $J(\mathbb{C}(x))$ est finie.*

Il existe alors une extension finie $K \subset \mathbb{C}$ de k_0 telle que tous les éléments de $J(\mathbb{C}(x))$ soient définis sur $K(x)$.

Démonstration.

Le corollaire 3.1.2 s'applique : le groupe $J(\mathbb{C}(x))$ est abélien de type fini. Soit $P =< u, v >$ un élément de $J(\mathbb{C}(x))$ Soient $(u_{i,j})_{(i,j)\in I_1} \in \mathbb{C}^{I_1}$ et $(v_{i,j})_{(i,j)\in I_2} \in \mathbb{C}^{I_2}$ les coefficients des polynômes u et v : ils sont définis par $u = \sum_{(i,j)\in I_1} u_{i,j}x^iy^j$ et $v = \sum_{(i,j)\in I_2} v_{i,j}x^iy^j$. Nous supposons pour l'instant qu'au moins un des $u_{i,j}$ ou un des $v_{i,j}$ n'est pas algébrique sur k_0.

Soit $A = k_0[(u_{i,j})_{(i,j)\in I_1}, (v_{i,j})_{(i,j)\in I_2}]$ la k_0-algèbre engendrée par les $u_{i,j}$ et les $v_{i,j}$. La k_0-algèbre A est de type fini et le lemme de normalisation de Noether affirme l'existence de $t_1, \cdots, t_n \in A$ algébriquement indépendants tels que A soit un $k_0[t_1, \cdots, t_n]$-module de type fini.

À tout n-uplet $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{C}^n$ nous associons le morphisme de ϕ_α : $\begin{array}{ccc} k_0[t_1, \cdots, t_n] & \longrightarrow & \mathbb{C} \\ Q(t_1, \cdots, t_n) & \longmapsto & B(\alpha_1, \cdots, \alpha_n) \end{array}$. L'anneau A est une extension finie de $k_0[t_1, \cdots, t_n]$. Nous notons $t_{n+1}, \cdots, t_{n+m}$ des éléments de A tels que $A = k_0[t_1, \cdots, t_{n+m}]$. Soit Q_i le polynôme minimal de t_i sur $k_0[t_1, \cdots, t_n]$. Le corps $\mathbb{C}$ est algébriquement clos. Les polynôme Q_i sont donc scindés sur $\mathbb{C}$. Ainsi, le morphisme ϕ_α s'étend en un morphisme de $\tilde{\phi}_\alpha : A \longrightarrow \mathbb{C}$. Nous notons $\Phi_\alpha : A(x)[y] \longrightarrow \mathbb{C}(x)[y]$ l'unique morphisme qui envoie x sur x, y sur y et dont la restriction à A est $\tilde{\phi}_\alpha$. Comme $u(y)$ divise $f(y) - (v(y))^2$, le polynôme $\Phi_\alpha(u)$ divise $\Phi_\alpha(f - v^2) = f - \Phi_\alpha(v^2)$. Ainsi, le couple $(\Phi_\alpha(u), \Phi_\alpha(v))$ est la représentation de Mumford d'un $\mathbb{C}(x)$-point P_α de J.

Soient $\alpha \in \mathbb{C}^n$ et $\beta \in \mathbb{C}^n$ deux n-uplets différents. Les morphismes ϕ_α et ϕ_β sont différents. Les morphismes $\tilde{\phi}_\alpha$ et $\tilde{\phi}_\beta$ sont donc différents. Comme A est la k_0-algèbre engendrée par les $u_{i,j}$ et les $v_{i,j}$, un des $u_{i,j}$ ou un des $v_{i,j}$ doit avoir une image par $\tilde{\phi}_\alpha$ différente de son image par $\tilde{\phi}_\beta$. Cela signifie que que $\Phi_\alpha(u) \neq \Phi_\beta(u)$ ou $\Phi_\alpha(v) \neq \Phi_\beta(v)$ c'est-à-dire que P_α et P_β sont distincts (par unicité de la représentation de Mumford d'un point de J).

Nous venons ainsi d'associer à P une infinité non dénombrable d'éléments de $J(\mathbb{C}(x))$ qui est pourtant de type fini. Cette contradiction signifie que les $u_{i,j}$ et les $v_{i,j}$ sont tous algébriques sur k_0. Ainsi, pour tout $\mathbb{C}(x)$-point P de J, il existe une extension finie K de k_0 tel que $P \in J(K(x))$.

Le groupe $J(\mathbb{C}(x))$ est abélien de type fini. Soit $\{P_1, \cdots, P_r\}$ un ensemble de générateurs de $J(\mathbb{C}(x))$. Soit K la plus petite extension de k_0 telle que les P_i soient tous des éléments de $J(K(x))$. Nous venons juste de montrer que cette extension K de k_0 est finie Puisque les P_i génèrent $J(\mathbb{C}(x))$, tout élément de $J(\mathbb{C}(x))$ est en fait élément de $J(K(x))$. □

Le gros défaut du corollaire 3.3.2.1 est que le corps K qu'il définit reste théorique. On peut cependant le préciser grâce à une proposition extraite de [Chr76] :

Proposition 3.3.2.2 *Soit Γ un groupe fini et $\mathcal{A}$ un groupe abélien libre de type fini muni d'une action du groupe Γ. On suppose que l'action induite de Γ sur $\mathcal{A}/2\mathcal{A}$ est triviale.*
Le groupe $\mathcal{A}$ possède alors une base $(a_i)_{i=1}^t$ telle que $\forall \sigma \in \Gamma, \sigma(a_i) \in \{-a_i, a_i\}$.

Lemme 3.3.2.3 *Nous conservons les notations et hypothèses de la proposition 3.3.2.2. Nous supposons de plus que l'action de Γ sur $\mathcal{A}$ est fidèle.*

Alors, le groupe Γ ne contient aucun élément d'ordre impair non trivial.

Démonstration.

Nous allons démontrer par récurrence sur m que, pour tout $m \in \mathbb{N}^*$, pour tout élément $\sigma \in \Gamma$ d'ordre impair et pour tout $a \in \mathcal{A}$, nous avons $a - \sigma(a) \in 2^m\mathcal{A}$.

Dans le cas $m = 1$, cette hypothèse de récurrence se traduit par : tous les éléments de Γ d'ordre impair agissent trivialement sur $\mathcal{A}/2\mathcal{A}$. Cette assertion est vraie par hypothèse.

Supposons l'hypothèse de récurrence vraie au rang m. Soit $\sigma \in \Gamma$ un élément d'ordre impair n. Soit a un élément de $\mathcal{A}$. Comme σ est d'ordre impair, il en va de même de $\tau := \sigma^{(n+1)/2}$. L'hypothèse de récurrence affirme donc l'existence d'un élément b de $\mathcal{A}$ tel que $a - \tau(a) = 2^m b$. Puisque $\tau^2 = \sigma$, nous pouvons désormais écrire

$$\begin{aligned} a - \sigma(a) &= a - \tau(a) + \tau(a) - \sigma(a) \\ &= a - \tau(a) + \tau(a) - \tau^2(a) \\ &= (a - \tau(a)) + \tau(a - \tau(a)) \\ &= 2^m b + \tau(2^m b) \\ &= 2^m b + 2^m b - 2^m b + 2^m \tau(b) \\ &= 2^{m+1} b - 2^m (b - \tau(b)). \end{aligned}$$

Ceci permet de conclure que $a - \sigma(a) \in 2^{m+1}\mathcal{A}$, puisque, par hypothèse de récurrence, $b - \tau(b)$ est un élément de $2\mathcal{A}$.

Nous venons ainsi de montrer que l'hypothèse de récurrence est vraie au rang $m + 1$ lorsqu'elle est vraie au rang m. Par récurrence, les éléments $a - \sigma(a)$ sont dans $2^{m+1}\mathcal{A}$ pour tous $m \in \mathbb{N}^*$, $\sigma \in \Gamma$ d'ordre impair et $a \in \mathcal{A}$.

Cette assertion peut être formulée différemment : si $\sigma \in \Gamma$ est d'ordre impair et si $a \in \mathcal{A}$, alors a appartient à $\bigcap_{m=1}^{\infty} 2^m\mathcal{A}$. Le groupe $\mathcal{A}$ étant abélien libre de type fini, l'intersection $\bigcap_{m=1}^{\infty} 2^m\mathcal{A}$ est égale à $\{0\}$. Nous avons ainsi montré que, si $\sigma \in \Gamma$ est d'ordre impair, les éléments a de $\mathcal{A}$ vérifient tous $a = \sigma(a)$. Ce n'est possible que si $\sigma = \mathrm{Id}$ (l'action de Γ sur $\mathcal{A}$ est fidèle) : Id est le seul élément de Γ d'ordre impair. $\square$

Lemme 3.3.2.4 *On conserve les notations et hypothèses de la proposition 3.3.2.3. Soit $\sigma \in \Gamma$ un élément d'ordre 2. On pose $\mathcal{A}_+ := \{a \in \mathcal{A} | a = \sigma(a)\}$ et $\mathcal{A}_- := \{a \in \mathcal{A} | a = -\sigma(a)\}$.*

On peut alors décomposer le groupe $\mathcal{A}$ sous la forme $\mathcal{A} = \mathcal{A}_+ \oplus \mathcal{A}_-$.

Démonstration.

Le groupe abélien $\mathcal{A}$ étant sans torsion, $\mathcal{A}_+ \bigcap \mathcal{A}_-$ est égal à $\{0\}$. Pour montrer le lemme, il suffit donc de vérifier que $\mathcal{A} = \mathcal{A}_+ + \mathcal{A}_-$

Soit $a \in \mathcal{A}$. L'élément σ agit trivialement sur $\mathcal{A}/2\mathcal{A}$. Il existe donc $b \in \mathcal{A}$ tel que $a - \sigma(a) = 2b$. Comme σ est d'ordre 2, on peut vérifier que

$$\sigma(2b) = \sigma(a - \sigma(a)) = \sigma(a) - a = -2b.$$

Or le groupe $\mathcal{A}$ est sans torsion, donc $\sigma(b) = -b$. Ainsi, b appartient à $\mathcal{A}_-$. Pour montrer le lemme, nous vérifions que $b + \sigma(a) \in \mathcal{A}_+$. Pour cela, nous utilisons l'égalité

$$2(b + \sigma(a)) = a - \sigma(a) + 2\sigma(a) = a + \sigma(a).$$

Comme σ est d'ordre 2, nous avons l'égalité

$$\sigma(2(b+\sigma(a))) = \sigma(a) + \sigma^2(a) = \sigma(a) + a = 2(b+\sigma(a)).$$

Le groupe $\mathcal{A}$ étant sans torsion, l'élément $b+\sigma(a)$ est σ-invariant. Ainsi,

$$a = a - \sigma(a) + \sigma(a) = 2b + \sigma(a) = (b+\sigma(a)) + b,$$

appartient à $\mathcal{A}_+ \oplus \mathcal{A}_-$. □

Lemme 3.3.2.5 *Nous conservons les notations et hypothèses de la proposition 3.3.2.3. Alors le groupe* Γ *est un groupe d'exposant* 2.

Démonstration.

Soit $\tau \in \Gamma$ un élément d'ordre 4. Nous posons $\sigma = \tau^2$. L'élément σ de Γ est d'ordre 2 ; le lemme 3.3.2.4 peut s'appliquer à σ : nous disposons d'une décomposition $\mathcal{A} = \mathcal{A}_+ \bigoplus \mathcal{A}_-$ avec $\mathcal{A}_+ := \{a \in \mathcal{A} | a = \sigma(a)\}$ et $\mathcal{A}_- := \{a \in \mathcal{A} | a = -\sigma(a)\}$. Si $\mathcal{A}_-$ est vide, alors $\mathcal{A}$ est égal à $\mathcal{A}_+$ et nous avons une contradiction avec la fidélité de l'action de Γ sur $\mathcal{A}$.

Le groupe $\mathcal{A}$ est abélien libre de type fini. Il en va donc de même pour $\mathcal{A}_-$. Par suite, $\mathcal{A}_-$ contient un élément a non divisible par 2. Le groupe Γ agissant trivialement sur $\mathcal{A}/2\mathcal{A}$, il doit exister deux éléments b, $c \in \mathcal{A}$ tels que $\tau(a) = a + 2b$ et $\tau(b) = b + 2c$. Nous pouvons alors réécrire la σ-anti-invariance de a comme suit :

$$-a = \sigma(a) = \tau(\tau(a)) = \tau(a+2b) = \tau(a) + 2\tau(b) = (a+2b) + 2(b+2c).$$

Nous montrons ainsi que $-2a = 4(b+c)$ c'est-à-dire $a = -2(b+c)$ (car $\mathcal{A}$ est sans torsion). Ceci contredit le choix de a : l'élément a n'est pas divisible par 2.

Le groupe Γ ne contient donc aucun élément d'ordre 4. D'après le lemme 3.3.2.3, le groupe Γ ne contient pas non plus d'élément d'ordre impair non trivial. Par conséquent, Γ est d'exposant 2. □

Démonstration de la proposition 3.3.2.2.

Nous notons Γ_0 le sous-groupe des éléments de Γ qui agissent trivialement sur $\mathcal{A}$. Quitte à remplacer Γ par Γ/Γ_0 (dont l'action sur $\mathcal{A}$ est fidèle), nous pouvons supposer que Γ agit fidèlement sur $\mathcal{A}$. Nous allons montrer le résultat par récurrence sur l'ordre n du groupe Γ.

Le cas $n = 1$ est direct puisque Γ est le groupe trivial : il agit donc trivialement sur $\mathcal{A}$.

Nous supposons que la proposition 3.3.2.2 a été prouvée pour tout groupe d'ordre inférieur ou égal à $n-1$, et que Γ est d'ordre n.

Le groupe Γ est d'exposant 2 (d'après le lemme 3.3.2.5) et admet donc un sous-groupe G d'indice 2. Soit σ un élément de Γ qui n'est pas dans

G. D'après le lemme 3.3.2.4 appliqué à σ, on dispose d'une décomposition $\mathcal{A} = \mathcal{A}_+ \bigoplus \mathcal{A}_-$ avec

$$\mathcal{A}_+ := \{a \in \mathcal{A} | a = \sigma(a)\} \text{ et } \mathcal{A}_- := \{a \in \mathcal{A} | a = -\sigma(a)\}.$$

Le groupe Γ est d'exposant 2. Il est donc abélien. Par suite, les groupes abéliens libres $\mathcal{A}_+$ et $\mathcal{A}_-$ sont stables sous l'action de G. De plus, Γ agit trivialement sur $\mathcal{A}/2\mathcal{A}$, donc les actions de G sur $\mathcal{A}_+/2\mathcal{A}_+$ et $\mathcal{A}_-/2\mathcal{A}_-$ sont triviales.

Le groupe G étant d'ordre inférieur à $n-1$, on peut appliquer la proposition 3.3.2.2 au cas de l'action de G sur $\mathcal{A}_+$ et au cas de l'action de G sur $\mathcal{A}_-$. On obtient ainsi une base $(a_i)_{i=1}^s$ de $\mathcal{A}_+$ et une base $(a_i)_{i=s+1}^t$ de $\mathcal{A}_-$ telles que $\tau(a_i) \in \{-a_i, a_i\}$ pour tout $\tau \in G$. Tout $\rho \in \Gamma$ est soit dans G soit de la forme $\rho = \sigma\tau$ avec $\tau \in G$: il vérifie donc $\rho(a_i) \in \{-a_i, a_i\}$ (car σ agit comme Id sur $\mathcal{A}_+$ et comme $-$Id sur $\mathcal{A}_-$). $\square$

Proposition 3.3.2.6 *Soit k un sous-corps de $\mathbb{R}$. Soient $f \in k(x)[y]$ un polynôme de degré $2g+1$ (avec $g \in \mathbb{N}$) et $\mathcal{C}$ la courbe hyperelliptique sur $k(x)$ d'équation affine $z^2 = f(y)$. Soit J la jacobienne de $\mathcal{C}$. Nous supposons que*

1. *la torsion 2-primaire de $J(\mathbb{C}(x))$ est finie, et*
2. *l'action de $Gal(\mathbb{C}/k)$ sur $J(\mathbb{C}(x))/2J(\mathbb{C}(x))$ est triviale.*

Pour tout $d \in k^\times$, nous notons $\mathcal{C}_d$ la courbe hyperelliptique sur $k(x)$ d'équation affine $z^2 = d^{2g+1} f(\frac{y}{d})$.

Alors, le rang de Mordell-Weil de $J(\mathbb{R}(x))$ est non nul si et seulement si il existe $d \in k$ strictement positif tel que $Jac(\mathcal{C}_d)$ soit de $k(x)$-rang de Mordell-Weil non nul.

Démonstration.

Nous avons supposé que la torsion 2-primaire de $J(\mathbb{C}(x)$ est finie. Le corollaire 3.3.2.1 affirme donc l'existence d'une extension finie $K \subset \mathbb{C}$ de k telle que tous les points $\mathbb{C}(x)$-rationnels de J soient en fait $K(x)$-rationnels. Nous appliquons la proposition 3.3.2.2 aux groupes $\mathcal{A} := J(K(x))/J(K(x))_{tors}$ et $\Gamma := \mathrm{Gal}(K/k)$.

Nous supposons dans un premier temps que le rang de Mordell-Weil de $J(\mathbb{R}(x))$ est non nul. Le groupe Γ est bien un groupe fini, car K est une extension finie. De plus, d'après le corollaire 3.1.2, le groupe $\mathcal{A}$ est un groupe abélien libre de type fini. La proposition 3.3.2.2 implique alors l'existence d'une base $(\alpha_i)_{i=1}^t$ de $\mathcal{A}$ telle que $\tau(\alpha_i) \in \{-\alpha_i, \alpha_i\}$ pour tout $\tau \in \Gamma$.

Soit σ la conjugaison complexe. Puisque $k \subset \mathbb{R}$, l'automorphisme σ appartient à $\Gamma = \mathrm{Gal}(\mathbb{C}/k)$. Comme $\tau(\alpha_i) \in \{-\alpha_i, \alpha_i\}$ pour tout $\tau \in \Gamma$, l'action du groupe Γ commute avec celle de σ. Par suite, l'action de Γ sur $\mathcal{A}$ induit par restriction une action de Γ sur le sous-groupe $\mathcal{A}^\sigma$ des éléments de $\mathcal{A}$ invariants sous σ.

Le groupe $\mathcal{A}$ étant abélien libre, nous avons $\mathcal{A}^\sigma \cap 2\mathcal{A} = 2\mathcal{A}^\sigma$. Ainsi, l'inclusion de $\mathcal{A}^\sigma$ dans $\mathcal{A}$ induit par passage au quotient une injection de $\mathcal{A}^\sigma/2\mathcal{A}^\sigma \hookrightarrow \mathcal{A}/2\mathcal{A}$. Or l'action de Γ sur $\mathcal{A}/2\mathcal{A}$ est triviale, donc le groupe Γ agit trivialement sur $\mathcal{A}^\sigma/2\mathcal{A}^\sigma$. Nous utilisons alors la proposition 3.3.2.2 : il existe une base $(a_i)_{i=1}^t$ de $\mathcal{A}^\sigma$ telle que $\forall \tau \in \Gamma, \tau(a_i) \in \{-a_i, a_i\}$.

Nous notons $P_i \in J(K(x))$ un représentant de a_i. Soit m l'exposant de $J(K(x))_{tors}$. Soit $\tau \in \Gamma$. Si $\tau(a_i) = a_i$, alors $\tau(P_i) - P_i$ est un point de torsion de J et donc mP_i est τ-invariant. Ainsi, dans le cas où $\tau(a_i) = a_i$ pour tout $\tau \in \Gamma$, le point mP_i est un élément d'ordre infini de $J(k(x)) = \mathrm{Jac}(\mathcal{C}_1)(k(x))$.

Nous supposons qu'il existe un élément $\tau_i \in \Gamma$ tel que $\tau_i(a_i) = -a_i$. Cela signifie que $P_i + \tau_i(P_i)$ est un élément de torsion de $J(K(x))$, et donc que $mP_i = -\tau_i(mP_i)$. De même, l'orbite de P_i sous l'action de Γ est contenue dans l'ensemble des $\pm P_i + T$ où T doit être un élément de torsion de $J(K(x))$. Ainsi, l'orbite de mP_i sous l'action de Γ est d'ordre exactement 2. Le stabilisateur Γ_i de mP_i sous l'action de Γ est donc d'indice 2. Par conséquent, le corps K^{Γ_i} des invariants de K sous l'action de Γ_i est une extension de degré 2 de k, c'est-à-dire qu'il existe $d_i \in k$ qui n'est pas un carré dans k tel que $K^{\Gamma_i} = k(\sqrt{d_i})$. Le point mP_i appartient à $J(K^{\Gamma_i}(x))$.

Comme $a_i \in \mathcal{A}^\sigma$ est invariant sous σ, la conjugaison complexe σ appartient à Γ_i. Par suite, $k(\sqrt{d_i}) \subset \mathbb{R}$, et donc $\sqrt{d_i}$ appartient à $\mathbb{R}$, c'est-à-dire que d_i est strictement positif.

Le polynôme f étant de degré impair, les courbes $\mathcal{C}$ et $\mathcal{C}_{d_i}$ ont un point $k(x)$-rationnel au dessus du point à l'infini de $\mathbb{P}^1$, et donc

* $\mathrm{Jac}(\mathcal{C})(K^{\Gamma_i}(x)) = \mathrm{Pic}^0(K^{\Gamma_i}(x)(\mathcal{C}))$,
* $\mathrm{Jac}(\mathcal{C})(k(x)) = \mathrm{Pic}^0(k(x)(\mathcal{C}))$ et
* $\mathrm{Jac}(\mathcal{C}_{d_i})(k(x)) = \mathrm{Pic}^0(k(x)(\mathcal{C}_{d_i}))$.

Nous notons $\iota : \begin{array}{ccc} K(x)(\mathcal{C}) & \longrightarrow & K(x)(\mathcal{C}) \\ A(y,z) & \longmapsto & A(y,-z) \end{array}$ l'involution hyperelliptique. Le sous-corps des éléments τ_i-invariants de $K^{\Gamma_i}(x)(\mathcal{C})$ est $k(x)(\mathcal{C})$. De plus, le morphisme $\phi : \begin{array}{ccc} k(x)(\mathcal{C}_{d_i}) & \longrightarrow & K^{\Gamma_i}(x)(\mathcal{C}) \\ A(s,t) & \longmapsto & A(d_i y, d_i^g \sqrt{d_i} z) \end{array}$ est à valeurs dans $K^{\Gamma_i}(x)(\mathcal{C})^{\iota\circ\tau_i}$. Le sous-corps $\mathrm{Im}(\phi)$ de $K^{\Gamma_i}(x)(\mathcal{C})$ est d'indice 2 (une base du $\mathrm{Im}(\phi)$-espace vectoriel $K^{\Gamma_i}(x)(\mathcal{C})$ est $(1, \sqrt{d_i})$). Par conséquent, $\mathrm{Im}(\phi)$ est égal à $K^{\Gamma_i}(x)(\mathcal{C})^{\iota\circ\tau_i}$. Comme $2mP_i$ est un élément d'ordre infini de $2\mathrm{Jac}(\mathcal{C})(K^{\Gamma_i}(x)) = 2\mathrm{Pic}^0(K^{\Gamma_i}(x)(\mathcal{C}))$, nous déduisons de la proposition 3.2.6 que le groupe

$$\mathrm{Pic}^0(k(x)(\mathcal{C})) \times \mathrm{Pic}^0(k(x)(\mathcal{C}_{d_i})) = \mathrm{Jac}(\mathcal{C}_1)(k(x)) \times \mathrm{Jac}(\mathcal{C}_{d_i})(k(x))$$

contient un élément d'ordre infini. Par suite, l'un des deux groupes $\mathrm{Jac}(\mathcal{C}_1)(k(x))$ ou $\mathrm{Jac}(\mathcal{C}_{d_i})(k(x))$ contient un élément d'ordre infini.

Nous supposons maintenant qu'il existe $d_i \in k$ strictement positif tel que $\mathrm{Jac}(\mathcal{C}_{d_i})(k(x))$ ai un élément a d'ordre infini. D'après la proposition 3.2.6, le morphisme de groupe

$$CN_{k(\sqrt{d_i})(x)(\mathcal{C})/k(x)(\mathcal{C}_{d_i})} : \mathrm{Jac}(\mathcal{C}_{d_i})(k(x)) \longrightarrow \mathrm{Jac}(\mathcal{C})(k(\sqrt{d_i})(x))$$

est de noyau fini. L'image de a par $CN_{K(\sqrt{d_i})(x)(\mathcal{C})/k(x)(\mathcal{C}_{d_i})}$ n'est donc pas de torsion. Ainsi, le groupe $\mathrm{Jac}(\mathcal{C})(k(\sqrt{d_i})(x))$ est de rang de Mordell-Weil supérieur ou égal à 1. Par suite, $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est de rang de Mordell-Weil supérieur ou égal à 1 (car, d_i étant strictement positif, nous avons $k(\sqrt{d_i}) \subset \mathbb{R}$). □

Nous terminons cette section en explicitant un cas où ce qui a été fait précédemment s'applique. Pour cela nous reprenons les notations 1.5.1.

Proposition 3.3.2.7 *Soit k un sous-corps de $\mathbb{R}$. Soient $f(y) \in k[x][y]$ un polynôme unitaire, de degré impair $2g+1$, sans facteur carré, et $\mathcal{C}$ la courbe hyperelliptique définie sur $k(x)$ par l'équation affine $z^2 = f(y)$. Nous supposons qu'il existe $2g$ éléments $e_1, \cdots, e_{2g-1}$, $H \in k[x]$ et un polynôme $\mu(y) \in k[x][y]$ tels que $f(y) = \mu(y) \prod_{i=1}^{2g-1} (y - He_i)$. Nous supposons de plus que :*

- *la torsion 2-primaire de $Jac(\mathcal{C})(\mathbb{C}(x))$ est finie*
- *le discriminant $\Delta(f)$ de $f(y)$ est scindé sur k,*
- *le discriminant $\Delta(\mu)$ de μ est de la forme H^2Q^2D avec $D \in k[x]$ un polynôme de degré 1 et $Q \in k[x]$,*
- *$\Delta(f) = Q^2Q_1$ avec $Q_1 \in k[x]$ premier à Q, et*
- *pour toute racine $\alpha \in k$ de H, l'élément $D(\alpha)$ est un carré dans k.*

Pour tout $d \in k^\times$, nous notons $\mathcal{C}_d$ la courbe hyperelliptique sur $k(x)$ d'équation affine $z^2 = d^{2g+1} f(\frac{y}{d})$.

Alors, le rang de Mordell-Weil de $Jac(\mathcal{C})(\mathbb{R}(x))$ est non nul, si et seulement si il existe $d \in k$ strictement positif tel que $Jac(\mathcal{C}_d)$ soit de $k(x)$-rang de Mordell-Weil non nul.

Démonstration.

Nous notons $\pi_{\mathcal{C}}$ le morphisme de Cassels-Schaefer associé à $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$. Le théorème 3.3.1.9 affirme que le groupe $\mathrm{Gal}(\mathbb{C}/k)$ agit trivialement sur l'image de $\pi_{\mathcal{C}}$. Par suite, le groupe $\mathrm{Gal}(\mathbb{C}/k)$ agit trivialement sur $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))/2\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$. Ainsi, nous sommes sous les hypothèses de la proposition 3.3.2.6. Par conséquent, le rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est non nul, si et seulement si il existe $d \in k$ strictement positif tel que $\mathrm{Jac}(\mathcal{C}_d)$ soit de $k(x)$-rang de Mordell-Weil non nul. □

3.4 Une traduction des conditions de descente en termes de coefficients

Nous nous intéressons dans cette partie à des polynômes sans facteur carré de la forme

$$P(y) = (y^2+1)(y^2+C(x^2))(y^4+(1+C(x^2))y^2+B(x^2))$$

où B, $C \in \mathbb{R}[x]$ sont des polynômes totalement positifs. Soit $\mathcal{C}$ la courbe hyperelliptique d'équation affine $z^2 + P(y) = 0$. Nous souhaitons montrer que le rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est nul.

À tout $\delta \in \mathbb{R}(x)^\times$ nous associons les $\mathbb{R}(x)$-courbes hyperelliptiques $\mathcal{C}_\delta^+$ et $\mathcal{C}_\delta^-$ d'équations affines respectives :

$\mathcal{C}_\delta^+ : z^2 = y(y-\delta)(y-\delta C(x))(y^2-\delta[1+C(x)]y+\delta^2 B(x))$ et
$\mathcal{C}_\delta^- : t^2 = s(s^2-\delta[(1-C(x))^2-2(B(x)-C(x))]s+\delta^2(B(x)-C(x))^2)$.

Nous supposons que les polynômes $B(x^2)$, $C(x^2)$, $B(x^2)C(x^2)$, $B(x^2)-C(x^2)$, $(B(x^2)-C(x^2))(1-C(x^2))$ et $(1+C(x^2))^2-4B(x^2)$ ne sont pas des carrés dans $\mathbb{C}(x)$. D'après le corollaire 3.2.10, le $\mathbb{R}(x)$-rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})$ est nul si et seulement si les jacobiennes des courbes $\mathcal{C}_1^+$, $\mathcal{C}_x^+$, $\mathcal{C}_1^-$ et $\mathcal{C}_x^-$ sont de $\mathbb{R}(x)$-rang de Mordell-Weil nuls

L'objet de cette section est de simplifier les calculs des $\mathbb{R}(x)$-rangs de Mordell-Weil des jacobiennes des courbes $\mathcal{C}_1^+$, $\mathcal{C}_x^+$, $\mathcal{C}_1^-$ et $\mathcal{C}_x^-$ en appliquant la proposition 3.3.2.7. Ceci impose de choisir judicieusement les coefficients de B, $C \in \mathbb{R}[x]$.

3.4.1 Une explicitation des conditions permettant la 2-descente.

Proposition 3.4.1.1 *Soient $B(x)$, $C(x) \in \mathbb{R}[x]$ deux polynômes. À tout $\delta \in k(x)^\times$ nous associons les $k(x)$-courbes hyperelliptiques $\mathcal{C}_\delta^+$ et $\mathcal{C}_\delta^-$ d'équations affines respectives :*

$\mathcal{C}_\delta^+ : z^2 = y(y-\delta)(y-\delta C(x))(y^2-\delta[1+C(x)]y+\delta^2 B(x))$ *et*
$\mathcal{C}_\delta^- : t^2 = s(s^2-\delta[(1-C(x))^2-2(B(x)-C(x))]s+\delta^2(B(x)-C(x))^2)$.

Soit k un sous corps de $\mathbb{R}$ contenant les coefficients de B et C. Nous supposons que

* *les polynômes $B(x^2)$, $C(x^2)$, $B(x^2)C(x^2)$, $B(x^2)-C(x^2)$, $(B(x^2)-C(x^2))(1-C(x^2))$ et $(1+C(x^2))^2-4B(x^2)$ ne sont pas des carrés dans $\mathbb{C}(x)$,*
* *les polynômes B, C, $B-C$ et $1-C$ sont scindés sur k,*
* *le polynôme $(1+C(x))^2-4B(x)$ est de degré 1 et son évaluation en 0 est un carré dans k.*
* *le polynôme $1-C$ est premier à x, B, $B-C$ et $(1+C)^2-4B$.*

Alors les $\mathbb{R}(x)$-rangs de Mordell-Weil de $Jac(\mathcal{C}_1^+)$, $Jac(\mathcal{C}_x^+)$, $Jac(\mathcal{C}_1^-)$ et $Jac(\mathcal{C}_x^-)$ sont nuls si et seulement si, pour tout élément strictement positif ζ de k, les $k(x)$-rangs de Mordell-Weil de $Jac(\mathcal{C}_\zeta^+)$, $Jac(\mathcal{C}_{\zeta x}^+)$, $Jac(\mathcal{C}_\zeta^-)$ et $Jac(\mathcal{C}_{\zeta x}^-)$ sont nuls.

Démonstration.

Soient ζ un élément strictement positif de k et $\delta \in \{\zeta, \zeta x\}$. Soit $\mathcal{C}$ la courbe hyperelliptique d'équation affine

$$\mathcal{C} : z^2 + (y^2+1)(y^2 + C(x^2))(y^4 + (1 + C(x^2))y^2 + B(x^2)) = 0.$$

D'après le corollaire 3.1.3 le groupe $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ est de type fini. Par conséquent les groupes $\mathrm{Jac}(\mathcal{C}_\zeta^+)(\mathbb{C}(x))$, $\mathrm{Jac}(\mathcal{C}_{\zeta x}^+)(\mathbb{C}(x))$, $\mathrm{Jac}(\mathcal{C}_\zeta^-)(\mathbb{C}(x))$ et $\mathrm{Jac}(\mathcal{C}_{\zeta x}^-)(\mathbb{C}(x))$ sont de type fini (voir les propositions 3.2.7 et 3.2.9).

Le discriminant du polynôme

$$g(s) := s^2 + \delta\left((1 - C(x))^2 - 2(B(x) - C(x))\right)s + \delta^2(B(x) - C(x))^2$$

est

$$\delta^2(1 - C(x))^2((1 + C(x))^2 - 4B(x))$$

et celui du polynôme $sg(s)$ est

$$\delta^6(B(x) - C(x))^4(1 - C(x))^2((1 + C(x))^2 - 4B(x)).$$

La proposition 3.3.2.7 s'applique donc à la courbe $\mathcal{C}_\delta^-$ et au corps k si les trois conditions suivantes sont vérifiées :

* les polynômes $(B(x) - C(x))$ et $(1 - C(x))$ sont scindés sur k.
* le polynôme $(1 + C(x))^2 - 4B(x)$ est de degré 1 et son évaluation en toute racine de δ est un carré dans k, et
* le polynôme $1 - C$ est premier à δ, $B - C$ et $(1 + C)^2 - 4B$.

De même, le discriminant de $y^2 - \delta(1 + C(x))y + \delta^2 B(x)$ est

$$\delta^2[(1 + C(x))^2 - 4B(x)],$$

et celui du polynôme

$$y(y - \delta)(y - \delta C(x))((y - \delta\frac{1 + C(x)}{2})^2 - \delta^2\frac{(1 + C(x))^2 - 4B(x)}{4})$$

est

$$\delta^{20}B(x)^2C(x)^2(C(x) - 1)^2(B(x) - C(x))^4((1 + C(x))^2 - 4B(x))),$$

donc la proposition 3.3.2.7 s'applique à la courbe $\mathcal{C}_\delta^+$ si

* les polynômes B, C, $B - C$ et $1 - C$ sont scindés sur k
* le polynôme $(1 + C)^2 - 4B$ est de degré 1 et son évaluation en toute racine de δ est un carré dans k. $\square$

3.4.2 La définition du corps de base

Dans cette sous-section, nous présentons un cas particulier de la proposition 3.4.1.1. Plus précisément nous choisissons les deux polynômes $B(x)$, $C(x) \in \mathbb{R}(x)$ de façon à simplifier au maximum le calcul, pour tout $\zeta \in k$ strictement positif, des $k(x)$-rangs de Mordell-Weil des jacobiennes des courbes $\mathcal{C}_\zeta^+$, $\mathcal{C}_{\zeta x}^+$, $\mathcal{C}_\zeta^-$ et $\mathcal{C}_{\zeta x}^-$ définies au cours de la proposition 3.4.1.1. En particulier, nous choisissons les coefficients B et C de degrés les plus bas possibles.

Dans le cas où B et C sont de degrés 1 en x, le polynôme

$$P(x,y) := (y^2+1)(y^2+C(x^2))(y^2+(C(x^2)+1)y+B(x^2))$$

est de degré 4 en x. Nous pouvons alors déterminer si $P(x,y)$ est une somme de 3 carrés dans $\mathbb{R}(x,y)$ en considérant la courbe elliptique sur $\mathbb{R}(y)$ d'équation de Weierstrass $z^2 = P(x,y)$. Nous étudions donc le cas où l'un des polynômes B et C est de degré au moins 2.

Afin de forcer le polynôme $(1+C(x))^2-4B(x)$ à être de degré au plus 1, nous choisissons $B(x)$ unitaire de degré 2 et $C(x)$ de degré 1 et de coefficient dominant 2.

Pour pouvoir appliquer la proposition 3.4.1.1, nous devons aussi nous assurer que B et $B-C$ sont scindés sur k, c'est-à-dire (puisque B et $B-C$ sont de degrés 2) que leurs discriminants sont des carrés dans k.

Nous nommons les coefficients des polynômes B et C en écrivant

$$B(x) =: (x+b_1)^2 + b_0 \text{ et } C(x) =: 2(x+b_1) + r.$$

Avec ces notations, le discriminant de B est $-4b_0$ et celui de

$$B - C = (x+b_1)^2 - 2(x+b_1) + b_0 - r$$

est $4-4b_0+4r$. Nous montrons ainsi que les polynômes B et $B-C$ sont scindés sur k si et seulement si il existe un couple (η,ω) tel que $-4b_0 = 4\eta^2$ et $4-4b_0+4r = 4\omega^2$, c'est-à-dire tel que

$$b_0 = -\eta^2 \text{ et } r = \omega^2 - \eta^2 - 1.$$

Nous supposons que c'est le cas. Le coefficient dominant du polynôme

$$\begin{aligned}(1+C)^2-4B &= (2x+2b_1+\omega^2-\eta^2)^2 - 4(x+b_1)^2 - 4b_0 \\ &= 4(\omega^2-\eta^2)(x+b_1) + (\omega^2-\eta^2)^2 + 4\eta^2\end{aligned}$$

est $4(\omega^2-\eta^2)$. Le polynôme $(1+C)^2-4B$ est donc de degré 1 si et seulement si ω^2 et η^2 sont différents.

Nous souhaitons de plus que $(1+C(0))^2-4B(0)$ soit un carré dans k, c'est-à-dire que nous voulons l'existence de $\rho \in k$ tel que

$$b_1 = \frac{\rho^2-\eta^2}{\omega^2-\eta^2} + \frac{\eta^2-\omega^2}{4}.$$

Par ailleurs, le polynôme $1-C = -2\left(x+b_1-1+\frac{\omega^2-\eta^2}{2}\right)$ est premier aux polynômes x, $B=(x+b_1)^2-\eta^2$, $(B-C)=(x+b_1-1)^2-\omega^2$ et $[(1+C)^2-4B] = 4(\omega^2-\eta^2)(x+b_1)+(\omega^2-\eta^2)^2+4\eta^2$ si et seulement si les éléments

* $-2b_1+2+\eta^2-\omega^2$,
* $\eta^2-\omega^2+2+2\eta$ et $\eta^2-\omega^2+2-2\eta$, et
* $\eta^2-\omega^2+2\omega$ et $\eta^2-\omega^2-2\omega$

sont non nuls. Dans ce qui suit, nous supposons que ces conditions sont vérifiées.

Nous donnons maintenant des conditions sur η, ω et ρ sous lesquelles les polynômes $(1+C(x^2))^2-4B(x^2)$, $B(x^2)$, $C(x^2)$, $B(x^2)C(x^2)$, $B(x^2)-C(x^2)$ et $(B(x^2)-C(x^2))(1-C(x^2))$ ne sont pas des carrés dans $\mathbb{C}(x)$.

Si $\rho \neq 0$, le polynôme $(1+C(x^2))^2-4B(x^2) = 4(\omega^2-\eta^2)x^2+4\rho^2$ est de degré 2 et sans facteur carré. Dans ce cas, le polynôme $(1+C(x^2))^2-4B(x^2)$ n'est pas un carré dans $\mathbb{C}(x)$.

De même, si $2b_1+\omega^2-\eta^2-1$ est non nul, alors le polynôme $C(x^2) = 2(x^2+b_1)+\omega^2-\eta^2-1$ est de degré 2 et sans facteur carré, et n'est donc pas un carré dans $\mathbb{C}(x)$.

Les polynômes $B(x^2)-C(x^2)$ et $1-C(x^2)$ sont premiers entre eux, car les polynômes $B-C$ et $1-C$ ont été supposés premiers entre eux.

Lorsque ω est non nul, les polynômes $x^2+b_1-1+\omega$ et $x^2+b_1-1-\omega$ sont premiers entre eux. Si de plus les éléments $b_1-1+\omega$ et $b_1-1-\omega$ sont non nuls, alors le polynôme

$$B(x^2)-C(x^2) = (x^2+b_1-1)^2-\omega^2$$

est sans facteur carré de degré 4. Dans ce cas les polynômes $B(x^2)-C(x^2)$ et $(B(x^2)-C(x^2))(1-C(x^2))$ ne sont pas des carrés dans $\mathbb{C}(x)$ (car les polynômes $B(x^2)-C(x^2)$ et $1-C(x^2)$ sont premiers entre eux).

De même, si η, $b_1-\eta$ et $b_1-\eta$ sont non nuls, alors

$$B(x^2) = (x^2+b_1)^2-\eta^2$$

est un polynôme de degré 4 sans facteur carré. Dans ce cas, $B(x^2)$ n'est pas un carré dans $\mathbb{C}(x)$.

Nous supposons ces trois conditions vérifiées. Nous supposons de plus que le reste

$$\frac{(\omega^2-\eta^2-1)^2}{4}-\eta^2$$

de la division euclidienne de $B(x^2)=(x^2+b_1)^2-\eta^2$ par

$$C(x^2)=2(x^2+b_1)+\omega^2-\eta^2-1$$

est non nul. Alors les polynômes $B(x^2)$ et $C(x^2)$ sont premiers entre eux. Par suite, le polynôme $B(x^2)C(x^2)$ n'est pas un carré dans $\mathbb{C}(x)$.

Finalement, en utilisant la proposition 3.4.1.1 et le corollaire 3.2.10, nous aboutissons à un résultat de 2-descente pour la jacobienne de la courbe $\mathcal{C}$:

Théorème 3.4.2.1 *Soient η, ω, $\rho\in\mathbb{R}$ des réels. Nous posons :*

$$b_1=\frac{\rho^2-\eta^2}{\omega^2-\eta^2}+\frac{\eta^2-\omega^2}{4}.$$

Soient $B(x):=(x+b_1)^2-\eta^2$ et $C(x):=2(x+b_1)+\omega^2-\eta^2-1$. Nous supposons que les éléments

* *η, ω, ρ et $\omega^2-\eta^2$,*
* *$2b_1-2+\omega^2-\eta^2$,*
* *$\eta^2-\omega^2+2+2\eta$ et $\eta^2-\omega^2+2-2\eta$,*
* *$\eta^2-\omega^2+2\omega$ et $\eta^2-\omega^2-2\omega$,*
* *$\omega^2-\eta^2-1+2\eta$ et $\omega^2-\eta^2-1-2\eta$,*
* *$2b_1+\omega^2-\eta^2-1$, $b_1+\eta$, $b_1-\eta$, $b_1-1+\omega$ et $b_1-1-\omega$*

sont non nuls.

Soit $\mathcal{C}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$z^2+(y^2+1)(y^2+C(x^2))(y^4+(1+C(x^2))y^2+B(x^2))=0.$$

À tout $\delta\in k(x)^\times$ nous associons les $k(x)$-courbes hyperelliptiques $\mathcal{C}_\delta^+$ et $\mathcal{C}_\delta^-$ d'équations respectives :

$$\mathcal{C}_\delta^+ : t^2=y(y-\delta)(y-\delta C(x))(y^2-\delta[1+C(x)]y+\delta^2B(x)) \text{ et}$$
$$\mathcal{C}_\delta^- : t^2=s\left(s^2+\delta\left[(1-C(x))^2-2(B(x)-C(x))\right]s+\delta^2[B(x)-C(x)]^2\right).$$

Alors le $\mathbb{R}(x)$-rang de Mordell-Weil de $Jac(\mathcal{C})$ est nul si et seulement si, pour tout $\zeta\in k$ strictement positif, les $k(x)$-rangs de Mordell-Weil de $Jac(\mathcal{C}_\zeta^+)$, $Jac(\mathcal{C}_{\zeta x}^+)$, $Jac(\mathcal{C}_\zeta^-)$ et $Jac(\mathcal{C}_{\zeta x}^-)$ sont nuls.

3.5 Le calcul de rangs de Mordell-Weil à l'aide d'isogénies de Richelot.

Cette partie est reprise de divers articles ou ouvrages : [CF96], [Sch95], [Sch98], [Sto01].

3.5.1 Le principe général

Proposition 3.5.1.1 *Soit K un corps de caractéristique 0. Soient J et $\widehat{J}$ deux variétés abéliennes sur K. Nous supposons que le groupe $J(K)$ est de type fini. Soient $\varphi : J \longrightarrow \widehat{J}$ et $\widehat{\varphi} : \widehat{J} \longrightarrow J$ deux isogénies telles que $\varphi \circ \widehat{\varphi}$ soit la multiplication par 2 dans $\widehat{J}$ et $\widehat{\varphi} \circ \varphi$ soit la multiplication par 2 dans J.*

Alors, le rang de Mordell-Weil de $J(K)$ est nul si et seulement si $J(K)/\widehat{\varphi}(\widehat{J}(K))$ et $\widehat{J}(K)/\varphi(J(K))$ sont engendrés respectivement par la torsion de $J(K)$ et par la torsion $\widehat{J}(K)$.

Démonstration.

Si G est un groupe abélien, Nous désignons par G_{tors} le sous-groupe des éléments de torsion de G.

Nous supposons tout d'abord que $J(K)/\widehat{\varphi}(\widehat{J}(K))$ et $\widehat{J}(K)/\varphi(J(K))$ sont engendrés respectivement par la torsion de $J(K)$ et par la torsion de $\widehat{J}(K)$. Le groupe $J(K)$ étant de type fini, Le groupe quotient $J(K)/J(K)_{tors}$ admet une $\mathbb{Z}$-base. Nous supposons par l'absurde que le rang de Mordell-Weil de $J(K)$ est non nul. Soit α un élément d'une $\mathbb{Z}$-base de $J(K)/J(K)_{tors}$. L'élément α n'est pas un double dans $J(K)/J(K)_{tors}$. Soit $P \in J(K)$ un représentant de la classe α.

Comme $J(K)/\widehat{\varphi}(\widehat{J}(K))$ est engendré par $J(K)_{tors}$, il existe un élément $Q \in \widehat{J}(K)$ et un élément $T_1 \in J(K)_{tors}$ tel que $P = T_1 + \widehat{\varphi}(Q)$. De même $\widehat{J}(K)/\varphi(J(K))$ est engendré par $\widehat{J}(K)_{tors}$, et il existe donc un élément $R \in J(K)$ et un élément de torsion $T_2 \in \widehat{J}(K)_{tors}$ tel que $Q = T_2 + \varphi(R)$.

Puisque $\widehat{\varphi}(T_2)$ est un point de torsion de $J(K)$, l'élément α est la classe de $2R = P - T_1 - \widehat{\varphi}(T_2)$ dans $J(K)/J(K)_{tors}$. Cependant, α étant un élément d'une $\mathbb{Z}$-base de $J(K)/J(K)_{tors}$, l'élément α n'est pas un double dans $J(K)/J(K)_{tors}$. De cette contradiction nous déduisons que $J(K)$ est de rang de Mordell-Weil nul.

La réciproque est obtenue en remarquant que $\widehat{J}(K)$ est de torsion lorsque $J(K)$ est de torsion (le morphisme $\widehat{\varphi} : \widehat{J} \longrightarrow J$ est une isogénie). □

3.5.2 Le cas des courbes elliptiques

Pour ces rappels, le lecteur peut consulter les livres suivants : [Sil94], [ST92], [Sil92], [Kna92].

Notations 3.5.2.1 Soient K un corps de caractéristique 0, et a, $b \in K$. Nous considérons la courbe elliptique $\mathcal{E}$ d'équation de Weierstrass

$$\mathcal{E} : z^2 = y(y^2 + ay + b).$$

Soit $\widehat{\mathcal{E}}$ la courbe elliptique d'équation de Weierstrass

$$\widehat{\mathcal{E}} : z^2 = y(y^2 - 2ay + a^2 - 4b).$$

Les éléments neutres des courbes elliptiques $\mathcal{E}$ et $\widehat{\mathcal{E}}$ sont respectivement désignés par $\mathcal{O}$ et par $\widehat{\mathcal{O}}$.

Nous définissons une isogénie $\varphi : \mathcal{E} \longrightarrow \widehat{\mathcal{E}}$ en posant

$$\varphi(y,z) := \left(y + a + \frac{b}{y}, z\left(\frac{y^2-b}{y^2}\right)\right)$$

si (x,y) est un point de $\mathcal{E}$ tel que y soit non nul, et en posant $\varphi((0,0)) := \varphi(\mathcal{O}) := \widehat{\mathcal{O}}$.

Par symétrie du rôle de $\mathcal{E}$ et $\widehat{\mathcal{E}}$ nous définissons une isogénie de la courbe $\widehat{\mathcal{E}}$ vers une courbe elliptique isomorphe à la courbe $\mathcal{E}$. Cette isogénie correspond à l'isogénie $\widehat{\varphi} : \widehat{\mathcal{E}} \longrightarrow \mathcal{E}$ obtenue en posant

$$\widehat{\varphi}(y,z) := \left(\frac{1}{4}\left(y + a + \frac{b}{y}\right), z\left(\frac{y^2-b}{8y^2}\right)\right)$$

si (x,y) est un point de $\widehat{\mathcal{E}}$ tel que y soit non nul, et $\varphi((0,0)) := \varphi(\widehat{\mathcal{O}}) := \mathcal{O}$. Les isogénies φ et $\widehat{\varphi}$ sont de degrés 2 et duales l'une de l'autre.

Nous supposons que $\mathcal{E}(K)$ est de type fini. D'après la proposition 3.5.1.1, la courbe elliptique $\mathcal{E}$ est de K-rang de Mordell-Weil nul si et seulement si $\mathcal{E}(K)/\widehat{\varphi}(\widehat{\mathcal{E}}(K))$ et $\widehat{\mathcal{E}}(K)/\varphi(\mathcal{E}(K))$ sont respectivement engendrés par les classes des éléments de torsion de $\mathcal{E}(K)$ et $\widehat{\mathcal{E}}(K)$.

Notations 3.5.2.2 Soit K un corps de caractéristique 0. Soit α, $\beta \in K$. Soit $\mathcal{D}$ la courbe elliptique sur K d'équation de Weierstrass $z^2 = y(y^2 + \alpha y + \beta)$. À la courbe elliptique $\mathcal{D}$ nous associons un morphisme de groupe $\gamma_{\mathcal{D}} : \mathcal{D}(K) \longrightarrow K^\times/K^{\times 2}$ en prenant

* $\gamma_{\mathcal{D}}((x,y))$ égal à la classe de x dans $K^\times/K^{\times 2}$ si x est non nul,
* $\gamma_{\mathcal{D}}((0,0))$ égal à la classe de β dans $K^\times/K^{\times 2}$, et
* $\gamma_{\mathcal{D}}(\mathcal{O})$ égal à la classe de 1 dans $K^\times/K^{\times 2}$.

Le morphisme de groupe $\gamma_{\mathcal{E}}$ a pour noyau l'image de $\gamma_{\mathcal{E}}$. Par suite, $\mathcal{E}(K)/\widehat{\varphi}(\widehat{\mathcal{E}}(K))$ est isomorphe à $\gamma_{\mathcal{E}}(\widehat{\mathcal{E}}(K))$. Nous avons donc équivalence entre :

* le groupe $\mathcal{E}(K)/\widehat{\varphi}(\widehat{\mathcal{E}}(K))$ est engendré par les classes des élément de torsion $\mathcal{E}(K)$, et
* l'image $\gamma_{\mathcal{E}}$ est engendré par $\gamma_{\mathcal{E}}(\mathcal{E}(K)_{tors})$ (avec $\mathcal{E}(K)_{tors}$ la torsion de $\mathcal{E}(K)$).

Cette remarque est encore valable en intervertissant $\mathcal{E}$ et $\widehat{\mathcal{E}}$ (et donc φ et $\widehat{\varphi}$). En appliquant la proposition 3.5.1.1, nous montrons donc la proposition :

Proposition 3.5.2.3 *Nous conservons les notations 3.5.2.1 et 3.5.2.2. Nous supposons que le groupe abélien $\mathcal{E}(K)$ est de type fini. Si G est un groupe abélien, nous notons G_{tors} le sous-groupe des éléments de torsion de G.*

Alors le rang de Mordell-Weil de $\mathcal{E}(K)$ est nul si et seulement si $\gamma_{\mathcal{E}}(\mathcal{E}(K)) = \gamma_{\mathcal{E}}(\mathcal{E}(K)_{tors})$ et $\gamma_{\widehat{\mathcal{E}}}(\widehat{\mathcal{E}}(K)) = \gamma_{\widehat{\mathcal{E}}}(\widehat{\mathcal{E}}(K)_{tors})$.

3.5.3 Le cas des courbes hyperelliptiques de genre 2.

Cette partie est reprise de [CF96]. Nous ne donnons que les énoncés qui nous seront utiles par la suite. Pour les preuves et les notions concernant les isogénies de Richelot, le lecteur peut consulter [CF96] ou [BM88].

Notations 3.5.3.1 Soit K un corps de caractéristique 0. Soit $G_i(y) = g_{i,2}y^2 + g_{i,1}(y) + g_{i,0} \in K[y]$ un polynôme de degré au plus 2. Soit $\mathcal{C}$ la courbe hyperelliptique sur K d'équation affine

$$\mathcal{C} : z^2 = G_1(y)G_2(y)G_3(y).$$

Nous posons :

* $\Delta := \det(g_{i,j})$,
* $L_1(y) := G_2'(y)G_3(y) - G_2(y)G_3'(y)$,
* $L_2(y) = G_3'(y)G_1(y) - G_3(y)G_1'(y)$ et
* $L_3(y) = G_1'(y)G_2(y) - G_1(y)G_2'(y)$.

Soit $\widehat{\mathcal{C}}$ la courbe hyperelliptique sur K d'équation affine

$$\widehat{\mathcal{C}} : \Delta\widehat{z}^2 = L_1(\widehat{y})L_2(\widehat{y})L_3(\widehat{y}).$$

Notations 3.5.3.2 *La correspondance $(2,2)$ entre les courbes hyperelliptiques $\mathcal{C}$ et $\widehat{\mathcal{C}}$ définie par la sous-courbe $\mathcal{Z} \subset \mathcal{C} \times \widehat{\mathcal{C}}$ d'équations*

$$\begin{cases} G_1(y)L_1(\widehat{y}) + G_2(y)L_2(\widehat{y}) = 0 \\ z\widehat{z} = (y - \widehat{y})G_1(y)L_1(\widehat{y}) \end{cases}$$

induit une isogénie $\varphi : Jac(\mathcal{C}) \longrightarrow Jac(\widehat{\mathcal{C}})$. Cette isogénie est appelée isogénie de Richelot. En intervertissant $\mathcal{C}$ et $\widehat{\mathcal{C}}$, nous définissons une isogénie de Richelot $\widehat{\varphi} : Jac(\widehat{\mathcal{C}}) \longrightarrow Jac(\mathcal{C})$.

Remarque :

Les composées $\widehat{\varphi} \circ \varphi$ et $\varphi \circ \widehat{\varphi}$ sont les multiplications par 2 de $\mathrm{Jac}(\mathcal{C})$ et $\mathrm{Jac}(\widehat{\mathcal{C}})$ respectivement. Nous allons appliquer la proposition 3.5.1.1 aux isogénies φ et $\widehat{\varphi}$.

Définition 3.5.3.3 *Nous conservons les notations 3.5.3.1. Soit $K_{i,\mathcal{C}} := K[T]/(G_i(T))$ (l'anneau $K_{i,\mathcal{C}}$ est soit un corps soit le produit $K \times K$).*

Nous définissons un morphisme $\Pi_{\mathcal{C}} : Jac(\mathcal{C})(K) \longrightarrow (K^\times/K^{\times 2})^3$ de la façon suivante : si $div(u,v) \in Div^0(K(\mathcal{C}))$ est un diviseur semi-réduit tel que u soit premier à G_i, et si α désigne la classe d'équivalence linéaire de $div(u,v)$, alors la i-ème coordonnée de $\Pi_{\mathcal{C}}(\alpha)$ est la classe de $N_{K_{i,\mathcal{C}}/K}((-1)^{\deg(u)}u(T))$ dans $K^\times/K^{\times 2}$ (avec $i = 1$, 2 ou 3).

Proposition 3.5.3.4 *Nous conservons les notations 3.5.3.1 et 3.5.3.2. Alors le noyau de $\Pi_{\mathcal{C}}$ est l'image $\widehat{\varphi}(Jac(\widehat{\mathcal{C}})(K))$.*

Démonstration.
Le lecteur se reportera à [CF96], équation 10.2.13. □

Remarque :
Les courbes $\mathcal{C}$ et $\widehat{\mathcal{C}}$ ont un rôle symétrique. En intervertissant ces deux courbes, nous définssons un morphisme $\Pi_{\widehat{\mathcal{C}}}$ de noyau égal à l'image $\varphi(\mathrm{Jac}(\mathcal{C})(K))$.

Corollaire 3.5.3.5 *Nous conservons les notations 3.5.3.1. Si G est un groupe abélien, nous notons G_{tors} le sous-groupe des éléments de torsion de G.*

Alors le rang de Mordell-Weil de $Jac(\mathcal{C})(K)$ est nul si et seulement si $\Pi_{\mathcal{C}}(Jac(\mathcal{C})(K)) = \Pi_{\mathcal{C}}(Jac(\mathcal{C})(K)_{tors})$ et $\Pi_{\widehat{\mathcal{C}}}(Jac(\widehat{\mathcal{C}})(K)) = \Pi_{\mathcal{C}}(Jac(\widehat{\mathcal{C}})(K)_{tors})$.

Démonstration.
D'après la proposition 3.5.3.4, les morphismes $\Pi_{\mathcal{C}}$ et $\Pi_{\widehat{\mathcal{C}}}$ définissent deux isomorphismes : entre $\mathrm{Jac}(\mathcal{C})(K)/\widehat{\varphi}(\mathrm{Jac}(\widehat{\mathcal{C}})(K))$ et l'image de $\Pi_{\mathcal{C}}$ d'une part, et entre $\mathrm{Jac}(\widehat{\mathcal{C}})(K)/\varphi(\mathrm{Jac}(\mathcal{C}))$ et l'image de $\Pi_{\widehat{\mathcal{C}}}$ d'autre part. Pour conclure, nous appliquons la proposition 3.5.1.1. □

Théorème 3.5.3.6 *Soient η, ω, $\rho \in \mathbb{R}$ des réels. Soit $k := \mathbb{Q}(\eta, \omega, \rho)$. Nous posons :*

$$b_1 = \frac{\rho^2 - \eta^2}{\omega^2 - \eta^2} + \frac{\eta^2 - \omega^2}{4}.$$

Soient $B(x) := (x + b_1)^2 - \eta^2$ et $C(x) := 2(x + b_1) + \omega^2 - \eta^2 - 1$. Nous supposons que les éléments

* *η, ω, ρ et $\omega^2 - \eta^2$,*
* *$2b_1 - 2 + \omega^2 - \eta^2$,*
* *$\eta^2 - \omega^2 + 2 + 2\eta$ et $\eta^2 - \omega^2 + 2 - 2\eta$,*
* *$\eta^2 - \omega^2 + 2\omega$ et $\eta^2 - \omega^2 - 2\omega$,*
* *$\omega^2 - \eta^2 - 1 + 2\eta$ et $\omega^2 - \eta^2 - 1 - 2\eta$,*
* *$2b_1 + \omega^2 - \eta^2 - 1$, $b_1 + \eta$, $b_1 - \eta$, $b_1 - 1 + \omega$ et $b_1 - 1 - \omega$*

sont non nuls.

Soit $\mathcal{C}$ la courbe hyperelliptique d'équation affine

$$\mathcal{C} : z^2 + (y^2 + 1)(y^2 + C(x^2))(y^4 + (1 + C(x^2))y^2 + B(x^2)) = 0.$$

À tout $\delta \in k(x)^\times$ nous associons les $k(x)$-courbes hyperelliptiques $\mathcal{C}_\delta^+$, $\widehat{\mathcal{C}}_\delta^+$, $\mathcal{C}_\delta^-$, $\widehat{\mathcal{C}}_\delta^-$ d'équations affines respectives :

$$\begin{aligned}
&\mathcal{C}_\delta^+ : z^2 = \left(y + \tfrac{\delta(1+C(x))}{2}\right)\left(y^2 - \left(\tfrac{\delta(1-C(x))}{2}\right)^2\right)\left(y^2 - \tfrac{\delta^2[(1+C(x))^2 - 4B(x)]}{4}\right)\\
&\widehat{\mathcal{C}}_\delta^+ : z^2 = (y + \delta(1 + C(x)))(y^2 - 4\delta^2 B(x))(y^2 - 4\delta^2 C(x))\\
&\mathcal{C}_\delta^- : z^2 = y(y^2 - \delta[(1 - C(x))^2 - 2(B(x) - C(x))]y + \delta^2(B(x) - C(x))^2)\\
&\widehat{\mathcal{C}}_\delta^- : t^2 = y(y + \delta(1 - C(x))^2)(y + \delta((1 - C(x))^2 - 4(B(x) - C(x)))).
\end{aligned}$$

Alors le $\mathbb{R}(x)$-rang de Mordell-Weil de la jacobienne de la courbe $\mathcal{C}$ est nul si et seulement si, pour tout $\zeta \in k$ strictement positif, les images des homomorphismes

$$\gamma_{\mathcal{C}_\zeta^-},\ \gamma_{\mathcal{C}_{\zeta x}^-},\ \gamma_{\widehat{\mathcal{C}}_\zeta^-},\ \gamma_{\widehat{\mathcal{C}}_{\zeta x}^-},\ \Pi_{\mathcal{C}_\zeta^+},\ \Pi_{\mathcal{C}_{\zeta x}^+},\ \Pi_{\widehat{\mathcal{C}}_\zeta^+} \text{ et } \Pi_{\widehat{\mathcal{C}}_{\zeta x}^+}$$

sont respectivement les images des points de torsion $k(x)$-rationnels de

$$\mathcal{C}_\zeta^-,\ \mathcal{C}_{\zeta x}^-,\ \widehat{\mathcal{C}}_\zeta^-,\ \widehat{\mathcal{C}}_{\zeta x}^-,\ Jac(\mathcal{C}_\zeta^+),\ Jac(\mathcal{C}_{\zeta x}^+),\ Jac(\widehat{\mathcal{C}}_\zeta^+) \text{ et } Jac(\widehat{\mathcal{C}}_{\zeta x}^+).$$

Démonstration.

Si G est un groupe abélien, nous notons G_{tors} le sous-groupe des éléments de torsion de G.

Nous nous donnons un polynôme $\delta \in k[x]$ et nous Posons

$$G_1(s) := s,\ G_2(s) := (s-\delta)(s-\delta C(x)) \text{ et } G_3(s) := s^2-\delta(1+C(x))s+\delta^2 B(x).$$

Soit $\mathcal{H}_\delta^+$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H}_\delta^+ : t^2 = G_1(s)G_2(s)G_3(s).$$

Suivant les notations 3.5.3.1, nous posons :

* $\Delta = \det \begin{pmatrix} 0 & 1 & 0 \\ \delta^2 C & -\delta(1+C) & 1 \\ \delta^2 B & -\delta(1+C) & 1 \end{pmatrix} = \delta^2(B-C),$
* $\begin{aligned} L_1(\widehat{y}) &:= G_2'G_3 - G_2G_3' \\ &= 2\delta^2(B-c)\widehat{y} + \delta^3((1+C)C-(1+C)B) \\ &= \delta^2(B-C)(2\widehat{y}-\delta(1+C)), \end{aligned}$
* $L_2(\widehat{y}) := G_3'G_1 - G_3G_1' = \widehat{y}^2 - \delta^2 B$, et
* $L_3(\widehat{y}) := G_1'G_2 - G_1G_2' = \delta^2 C - \widehat{y}^2.$

La courbe hyperelliptique sur $k(x)$ d'équation affine

$$\Delta\widehat{z}^2 = L_1(\widehat{y})L_2(\widehat{y})L_3(\widehat{y})$$

est isomorphe à la courbe $\widehat{\mathcal{C}}_\delta^+$ (via le changement de variable $z := 4\widehat{z}$ et $y := -2\widehat{y}$). Ainsi, d'après la proposition 3.5.3.5, le rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{H}_\delta^+)(k(x))$ est nul si et seulement si

* $\Pi_{\mathcal{H}_\delta^+}(\mathrm{Jac}(\mathcal{H}_\delta^+)(k(x))) = \Pi_{\mathcal{H}_\delta^+}(\mathrm{Jac}(\mathcal{H}_\delta^+)(k(x))_{tors})$, et
* $\Pi_{\widehat{\mathcal{C}}_\delta^+}(\mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)(k(x))) = \Pi_{\widehat{\mathcal{C}}_\delta^+}(\mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)(k(x))_{tors})$.

Dans le critère ci-dessus nous souhaitons maintenant remplacer la courbe $\mathcal{H}_\delta^+$ par la courbe $\mathcal{C}_\delta^+$. La courbe $\mathcal{H}_\delta^+$ est isomorphe sur $k(x)$ à la courbe hyperelliptique $\mathcal{C}_\delta^+$ via le changement de variable $y := s - \frac{\delta(1+C)}{2}$. Ce changement de variables induit un isomorphisme de groupe $\Psi : \mathrm{Jac}(\mathcal{C}_\delta^+) \longrightarrow \mathrm{Jac}(\mathcal{H}_\delta^+)$.

De plus, l'image de $\Pi_{\mathcal{C}_\delta^+}$ est engendrée par l'image des point de torsion de $\mathrm{Jac}(\mathcal{C}_\delta^+)$ si et seulement si l'image de $\Pi_{\mathcal{H}_\delta^+} = \Pi_{\mathcal{C}_\delta^+} \circ \Psi^{-1}$ est engendrée par l'image des points de torsion de $\mathrm{Jac}(\mathcal{H}_\delta^+)$. Par suite, le rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C}_\delta^+)(k(x))$ est nul si et seulement si

* $\Pi_{\mathcal{C}_\delta^+}(\mathrm{Jac}(\mathcal{C}_\delta^+)((k(x)))) = \Pi_{\mathcal{C}_\delta^+}(\mathrm{Jac}(\mathcal{C}_\delta^+)((k(x)))_{tors})$, et
* $\Pi_{\widehat{\mathcal{C}}_\delta^+}(\mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)((k(x)))) = \Pi_{\widehat{\mathcal{C}}_\delta^+}(\mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)((k(x)))_{tors})$.

Nous concluons en appliquant les propositions 3.4.2.1 et 3.5.2.3. $\square$

Chapitre 4

Une famille de polynômes positifs ou nuls sur $\mathbb{R}^2$ qui ne sont pas somme de trois carrés dans $\mathbb{R}(x, y)$.

Nous rappelons tout d'abord la forme générale des polynômes étudiés dans ce chapitre. Soient η, ω, $\rho \in \mathbb{R}$ des réels. Soit $k := \mathbb{Q}(\eta, \omega, \rho)$. Nous posons :

$$b_1 = \frac{\rho^2 - \eta^2}{\omega^2 - \eta^2} + \frac{\eta^2 - \omega^2}{4}.$$

Soient $B(x) := (x + b_1)^2 - \eta^2$ et $C(x) := 2(x + b_1) + \omega^2 - \eta^2 - 1$.

Le but de ce chapitre est de trouver des conditions sous lesquelles le polynôme

$$P(x, y) = \left(y^2 + 1\right)\left(y^2 + C\left(x^2\right)\right)\left(y^4 + \left(1 + C\left(x^2\right)\right)y^2 + B\left(x^2\right)\right)$$

est positif ou nul sur $\mathbb{R}^2$ mais n'est pas une somme de trois carrés.
Soit $\mathcal{C}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{C} : z^2 + P(x, y) = 0.$$

Nous supposons que les éléments

* η, ω, ρ et $\omega^2 - \eta^2$,
* $2b_1 - 2 + \omega^2 - \eta^2$,
* $\left(\eta^2 - \omega^2 + 2\right)^2 - 4\eta^2 = \left(\eta^2 - \omega^2 + 2 + 2\eta\right)\left(\eta^2 - \omega^2 + 2 - 2\eta\right)$,
* $\left(\eta^2 - \omega^2\right)^2 - 4\omega^2 = \left(\eta^2 - \omega^2 + 2\omega\right)\left(\eta^2 - \omega^2 - 2\omega\right)$,
* $\omega^2 - \eta^2 - 1 + 2\eta$ et $\omega^2 - \eta^2 - 1 - 2\eta$,
* $2b_1 + \omega^2 - \eta^2 - 1$, $b_1 + \eta$, $b_1 - \eta$, $b_1 - 1 + \omega$ et $b_1 - 1 - \omega$

sont non nuls. Alors, d'après le corollaire 2.4.9, la jacobienne $\mathrm{Jac}(\mathcal{C})$ n'a aucun $\mathbb{R}(x)$-point de torsion antineutre. L'objet de ce chapitre est de montrer que $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est de rang de Mordell-Weil nul : dans ce cas, $\mathrm{Jac}(\mathcal{C})$ n'a aucun $\mathbb{R}(x)$-point antineutre, et donc P n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$. Pour cela nous utilisons le théorème 3.5.3.6.

À tout $\delta \in k(x)^\times$ nous associons les $k(x)$-courbes hyperelliptiques $\mathcal{C}_\delta^+$, $\widehat{\mathcal{C}}_\delta^+$, $\mathcal{C}_\delta^-$, $\widehat{\mathcal{C}}_\delta^-$ d'équations affines respectives :

$$\mathcal{C}_\delta^+ : z^2 = \left(y + \tfrac{\delta(1+C(x))}{2}\right)\left(y^2 - \left(\tfrac{\delta(1-C(x))}{2}\right)^2\right)\left(y^2 - \tfrac{\delta^2[(1+C(x))^2-4B(x)]}{4}\right)$$

$$\widehat{\mathcal{C}}_\delta^+ : z^2 = \left(y + \delta\left(1 + C\left(x\right)\right)\right)\left(y^2 - 4\delta^2 B\left(x\right)\right)\left(y^2 - 4\delta^2 C\left(x\right)\right)$$

$$\mathcal{C}_\delta^- : z^2 = y\left(y^2 - \delta\left[\left(1 - C\left(x\right)\right)^2 - 2\left(B\left(x\right) - C\left(x\right)\right)\right]y + \delta^2\left(B\left(x\right) - C\left(x\right)\right)^2\right)$$

$$\widehat{\mathcal{C}}_\delta^- : t^2 = y\left(y + \delta\left(1 - C\left(x\right)\right)^2\right)\left(y + \delta\left[\left(1 - C\left(x\right)\right)^2 - 4\left(B\left(x\right) - C\left(x\right)\right)\right]\right).$$

Notations 4.1 Si $\alpha, \beta \in k(x)^\times$ sont deux fractions rationnelles non nulles, nous disons que α et β sont équivalentes modulo les carrés et nous notons $\alpha \sim \beta$ s'il existe $\gamma \in k(x)^\times$ telle que $\alpha = \gamma^2\beta$. Nous notons $[a]$ la classe d'équivalence d'un élément a de $k(x)^\times$ pour la relation $\sim$.

Soit $P \in k[x]$ un polynôme irréductible. Si $\alpha, \beta \in k[x]$ sont deux polynômes non divisibles par P, nous disons que α et β sont équivalents modulo les carrés et modulo P, et nous notons $\alpha \sim \beta \bmod P$, s'il existe $\gamma_1, \gamma_2 \in k[x]$ non divisibles par P tels que $\gamma_1^2\alpha \equiv \gamma_2^2\beta \bmod P$.

Nous reprenons les définitions introduites dans la section 3.5.

Notations 4.2 Soit k un corps de caractéristique 0. Soient $\alpha \in k[x]$ et $\beta \in k[x]$ deux polynômes tels que $\beta(\alpha^2 - 4\beta) \neq 0$. Soit $\mathcal{E}$ la courbe elliptique sur $k(x)$ d'équation affine

$$\mathcal{E} : t^2 = s(s^2 + \alpha s + \beta).$$

Soit $\mathcal{O}$ l'élément neutre de $\mathcal{E}(k(x))$. Nous définissons un morphisme

$$\gamma_{\mathcal{E}} : \mathcal{E}(k(x)) \longrightarrow k(x)^\times / k(x)^{\times 2}$$

en posant $\gamma_{\mathcal{E}}(s,t) := [s]$ si $s \neq 0$, $\gamma_{\mathcal{E}}(0,0) := [\beta]$ et $\gamma_{\mathcal{E}}(\mathcal{O}) := [1]$. Nous notons aussi $\gamma_{\mathcal{E},k(x)}$ le morphisme $\gamma_{\mathcal{E}}$ lorsque nous souhaitons préciser le corps de base.

Notations 4.3 Soit k un corps de caractéristique 0. Soient $G_1(y) \in k(x)[y]$ un polynôme de degré 1 en y, et $G_2(y)$, $G_3(y) \in k(x)[y]$ deux polynômes de degrés 2 en y (pas nécessairement irréductibles).

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = G_1(y)G_2(y)G_3(y).$$

Soient $A_i := k(x)[y]/(G_i(y))$ et y_i la classe de y dans A_i. Nous notons

$$\Pi_{\mathcal{H}} : \mathrm{Jac}(\mathcal{H})(k(x)) \longrightarrow (k(x)^\times/k(x)^{\times 2})^3$$

l'unique morphisme dont la i-ème coordonnée envoie la classe d'équivalence linéaire d'un diviseur semi-réduit $\mathrm{div}(u,v)$ sur $\mathcal{H}$ tel que u soit premier à $G_i(y)$ sur la classe dans $k(x)^\times/k(x)^{\times 2}$ de $N_{A_{i,\mathcal{H}}/k(x)}\left((-1)^{\deg(u)}\, u\,(y_i)\right)$.

Notations 4.4 Soit k un corps de caractéristique 0. Soit $\delta \in k(x)^\times$. Nous précisons l'utilisation des notations 4.3 dans deux cas particuliers.

Lorsque $\mathcal{H} = \mathcal{C}_\delta^+$ est la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{C}_\delta^+ : z^2 = \left(y + \tfrac{\delta(1+C(x))}{2}\right)\left(y^2 - \left(\tfrac{\delta(1-C(x))}{2}\right)^2\right)\left(y^2 - \tfrac{\delta^2[(1+C(x))^2-4B(x)]}{4}\right),$$

nous utilisons les notations 4.3 en posant

$$G_1(y) := y + \tfrac{\delta(1+C(x))}{2}$$

$$G_2(y) := y^2 - \left(\tfrac{\delta(1-C(x))}{2}\right)^2 \text{ et}$$

$$G_3(y) := y^2 - \tfrac{\delta^2[(1+C(x))^2-4B(x)]}{4}.$$

Lorsque $\mathcal{H} = \widehat{\mathcal{C}}_\delta^+$ est la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\widehat{\mathcal{C}}_\delta^+ : z^2 = \left(y - \delta\left(1 + C\left(x\right)\right)\right)\left(y^2 - 4\delta^2 B\left(x\right)\right)\left(y^2 - 4\delta^2 C\left(x\right)\right),$$

nous utilisons les même notations 4.3 en posant

$$G_1(y) := y - \delta\left(1 + C\left(x\right)\right)$$

$$G_2(y) := y^2 - 4\delta^2 B\left(x\right) \text{ et}$$

$$G_3(y) := y^2 - 4\delta^2 C\left(x\right).$$

Les notations 4.2, 4.3 et 4.4, nous permettent d'énoncer la conclusion du théorème 3.5.3.6 : le $\mathbb{R}(x)$-rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})$ est nul si et seulement si, pour tout $\zeta \in k$ strictement positif, les images des homomorphismes

$$\gamma_{\mathcal{C}_\zeta^-},\ \gamma_{\mathcal{C}_{\zeta x}^-},\ \gamma_{\widehat{\mathcal{C}}_\zeta^-},\ \gamma_{\widehat{\mathcal{C}}_{\zeta x}^-},\ \Pi_{\mathcal{C}_\zeta^+},\ \Pi_{\mathcal{C}_{\zeta x}^+},\ \Pi_{\widehat{\mathcal{C}}_\zeta^+} \text{ et } \Pi_{\widehat{\mathcal{C}}_{\zeta x}^+}$$

sont respectivement les images des points de torsion $k(x)$-rationnels de

$$\mathcal{C}_{\zeta}^{-},\ \mathcal{C}_{\zeta x}^{-},\ \widehat{\mathcal{C}}_{\zeta}^{-},\ \widehat{\mathcal{C}}_{\zeta x}^{-},\ \mathrm{Jac}(\mathcal{C}_{\zeta}^{+}),\ \mathrm{Jac}(\mathcal{C}_{\zeta x}^{+}),\ \mathrm{Jac}(\widehat{\mathcal{C}}_{\zeta}^{+}) \text{ et } \mathrm{Jac}(\widehat{\mathcal{C}}_{\zeta x}^{+}).$$

Au cours de ce chapitre, nous étudions, dans quatre section distinctes, l'image des quatre morphismes $\gamma_{\mathcal{C}_{\delta}^{-}}$, $\gamma_{\widehat{\mathcal{C}}_{\delta}^{-}}$, $\Pi_{\mathcal{C}_{\delta}^{+}}$ et $\Pi_{\widehat{\mathcal{C}}_{\delta}^{+}}$. De ces études, nous déduisons des conditions sur η, ω et ρ sous lesquelles le $\mathbb{R}(x)$-rang de Mordell-Weil de $\mathrm{Jac}(\mathcal{C})$ est nul.

4.1 La méthode générale de l'étude.

Notations 4.1.1 Soit k un corps de caractéristique 0. Soit $f(y) \in k(x)[y]$ un polynôme unitaire sans facteur carré de degré impair. Nous considérons la courbe hyperelliptique $\mathcal{H}$ sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = f(y).$$

Soit $f = \prod_{i=1}^{r} P_i(y)$ la décomposition de f en facteurs premiers dans $k(x)[y]$. Soit $M := k(x)[t]/f(t)$. Soient $K_i := k(x)[y]/P_i(y)$ et y_i la classe de y dans K_i.

Nous notons $J_{\mathcal{H}} := \mathrm{Jac}(\mathcal{H})$. Soit $\pi_{\mathcal{H}} : J_{\mathcal{H}}(k(x)) \longrightarrow M^{\times}/M^{\times 2}$ le morphisme de Cassels-Schaefer associé à la courbe $\mathcal{H}$ et au corps $k(x)$. Grâce au lemme chinois, le morphisme $\pi_{\mathcal{H}}$ peut être vu comme un morphisme $\pi_{\mathcal{H}} : J_{\mathcal{H}}(k(x)) \longrightarrow \prod_{i=1}^{r} K_i^{\times}/K_i^{\times 2}$.

Notations 4.1.2 Dans ce qui suit nous notons $\pi_{\mathcal{H},i} : J_{\mathcal{H}}(k(x)) \longrightarrow K_i^{\times}/K_i^{\times 2}$ la i-ème coordonnée de $\pi_{\mathcal{H}}$.

La norme $N_{K_i/k(x)}$ de l'extension $K_i/k(x)$ induit un homomorphisme $N_{K_i/k(x)} : K_i^{\times}/K_i^{\times 2} \longrightarrow k(x)^{\times}/k(x)^{\times 2}$. Nous posons $\Xi_{\mathcal{H},i} := N_{K_i/k(x)} \circ \pi_{\mathcal{H},i}$.

Nous notons $\Xi_{\mathcal{H}} : J_{\mathcal{H}}(k(x)) \longrightarrow \prod_{i=1}^{r} k(x)^{\times}/k(x)^{\times 2}$ l'homomorphisme de i-ème coordonnée $\Xi_{\mathcal{H},i}$.

Soient $\zeta \in k^{\times}$ strictement positif. Nous supposons $\mathcal{H} \in \{\mathcal{C}_{\zeta}^{+}, \mathcal{C}_{\zeta x}^{+}, \widehat{\mathcal{C}}_{\zeta}^{+}, \widehat{\mathcal{C}}_{\delta}^{+}\}$. Nous souhaitons montrer que $\mathrm{Im}(\Pi_{\mathcal{H}})$ est égale à l'image du sous-groupe de torsion de $\mathrm{Jac}(\mathcal{H})(k(x))$ par $\Pi_{\mathcal{H}}$. Pour cela, nous étudions l'image de $\Xi_{\mathcal{H}}$. Nous en déduisons ensuite des renseignements sur l'image de $\Pi_{\mathcal{H}}$. Étudier d'abord le morphisme $\Xi_{\mathcal{H}}$ permet une étude plus précise de l'image de $\Pi_{\mathcal{H}}$. En effet les composantes de $\Pi_{\mathcal{H}}$ s'obtiennent à partir des composantes de $\Xi_{\mathcal{H}}$.

Par ailleurs, si $f(y)$ est de la forme $f(y) = y(y^2 + \alpha y + \beta)$ (avec α, $\beta \in k(x)$ tels que $\beta\left(\alpha^2 - 4\beta\right) \neq 0$), alors $\gamma_{\mathcal{H}}$ est la coordonnée de $\Xi_{\mathcal{H}}$ associée au facteur premier y du polynôme $y(y^2 + \alpha y + \beta)$.

La première étape de notre étude consiste à utiliser les équations de $\mathrm{Jac}(\mathcal{H})$ obtenues grâce à la représentation de Mumford (c.f. [Mum84]). Plus précisément nous utilisons l'assertion suivante : si $\mathrm{div}(u, v) \in \mathrm{Div}^0(k(x)(\mathcal{H}))$ est un diviseur semi-réduit, alors

$$f \equiv v^2 \bmod u.$$

Cette congruence, nous a précédemment permis de montrer les propositions 1.5.9 et 3.3.1.3. En associant ces deux propositions, nous obtenons la proposition :

Proposition 4.1.3 *Nous conservons les notations 4.1.1 et 4.1.2. Soit $i \in \{1, \cdots, r\}$. Pour tout $j \neq i$, nous posons*

$$d_{i,j} := pgcd\left(N_{K_i/k(x)}\left(P_i'(y_i)\prod_{k\neq i} P_k(y_i)\right), N_{K_j/k(x)}\left(P_j'(y_j)\prod_{k\neq j} P_k(y_j)\right)\right).$$

Soit $div(u, v)$ un diviseur semi-réduit de $k(x)(\mathcal{H})$. Nous notons $Cl(div(u, v)) \in Jac(\mathcal{H})(k(x))$ sa classe d'équivalence linéaire.

Il existe alors une famille $(\mu_{i,j})_{\substack{1 \leq i \leq r,\\ j \neq i}}$ d'éléments de $k[x]$ sans facteur carré telle que

* *les facteurs premiers de $\mu_{i,j}$ soient des facteurs premiers de $d_{i,j}$,*
* *$\mu_{i,j} = \mu_{j,i}$, et*
* *$\Xi_{\mathcal{H},i}(Cl(div(u, v)))$ soit la classe de $\prod_{j\neq i} \mu_{i,j}$.*

Démonstration.

Nous pouvons sans perte de généralité supposer que u est premier à f : tout diviseur sur $\mathcal{H}$ est linéairement équivalent à un diviseur semi-réduit $\mathrm{div}(u, v)$ avec u premier à f.

Le corps K_i est un corps de fonction sur k. Le corps K_i est donc le corps des fractions d'un anneau de Dedekind $\mathcal{O}_i$. Nous notons $(\mathcal{P}_{i,l})_{l\in I}$ la famille des idéaux premiers de $\mathcal{O}_i$ en lesquels $(-1)^{\deg(u)}u(y_i)$ a une valuation impaire et $(\mathcal{Q}_{i,l})_{l\in\widetilde{I}}$ la famille des idéaux en lesquels $(-1)^{\deg(u)}u(y_i)$ a une valuation paire. Pour tout indice $l \in I$ nous notons $n_l \in \mathbb{Z}$ l'unique entier tel que $v_{\mathcal{P}_{i,l}}(u) = 2n_l + 1$. De même pour tout indice $l \in \widetilde{I}$ nous notons $m_l \in \mathbb{Z}$ l'unique entier tel que $v_{\mathcal{Q}_{i,l}}(u) = 2m_l$. La décomposition en idéaux premiers de l'idéal associé à $(-1)^{\deg(u)}u(y_i)$ est

$$\left((-1)^{\deg(u)}u(y_i)\right) = \prod_{l\in I} \mathcal{P}_{i,l}^{2n_l+1} \times \prod_{l\in\widetilde{I}} \mathcal{Q}_{i,l}^{2m_l}$$

En appliquant $N_{K_i/k(x)}$, nous obtenons $N_{K_i/k(x)}((-1)^{\deg(u)}u(y_i)) = \beta_i\theta_i^2$ avec :

* $\beta_i \in k[x]$ un représentant de l'idéal $\prod_{l\in I} N_{K_i/k(x)}(\mathcal{P}_{i,l})$, et
* $\theta_i \in k(x)$ un représentant de $\prod_{l\in I} N_{K_i/k(x)}(\mathcal{P}_{i,l})^{n_l} \times \prod_{l\in \widetilde{I}} N_{K_i/k(x)}(\mathcal{Q}_{i,l})^{m_l}$.

Soient $\alpha_i \in k[x]$ un polynôme sans facteur carré et $\gamma_i \in k(x)$ tels que $\beta_i = \alpha_i\gamma_i^2$. Nous rappelons que $\pi_{\mathcal{H},i}(\mathrm{Cl}(\mathrm{div}(u,v))$ est la classe de $(-1)^{\deg(u)}u(y_i)$ dans $K_i^\times/K_i^{\times 2}$. L'image $\Xi_{\mathcal{H},i}(\mathrm{Cl}(\mathrm{div}(u,v)) = N_{K_i/k(x)}(\pi_{\mathcal{H},i}(\mathrm{Cl}(\mathrm{div}(u,v))))$ est donc égale à la classe de α_i dans $k(x)^\times/k(x)^{\times 2}$.

Soit ϵ_i le coefficient dominant de α_i. Nous définissons $\mu_{i,j}$ comme un plus grand commun diviseur de α_i et α_j avec le choix de coefficient dominant $\epsilon_{i,j}$ (de $\mu_{i,j}$) suivant :

* si $j \notin \{i-1, i, i+1\}$, nous choisissons $\mu_{i,j}$ unitaire ;
* nous prenons $\epsilon_{1,2}$ et $\epsilon_{2,1}$ égaux à ϵ_1 ;
* par récurrence sur i, nous posons $\epsilon_{i,i+1} := \frac{\epsilon_i}{\epsilon_{i-1,i}}$ puis $\epsilon_{i+1,i} := \epsilon_{i,i+1}$.

Par construction, nous avons $\epsilon_{i,i-1}\epsilon_{i,i+1} := \frac{\epsilon_{i,i-1}\epsilon_i}{\epsilon_{i-1,i}} = \epsilon_i$. Ainsi les polynômes α_i et $\prod_{j\neq i}\mu_{i,j}$ ont même coefficient dominant (et ce coefficient dominant est ϵ_i).

Il existe un polynôme sans facteur carré $\Lambda_i \in k[x]$ et un polynôme unitaire $\Gamma_i \in k[x]$ tels que $\prod_{j\neq i}\mu_{i,j} = \Lambda_i\Gamma_i^2$. Le coefficient dominant de Λ_i est ϵ_i.

L'image de $\pi_{\mathcal{H}}$ est contenue dans le noyau de l'application $M^\times/M^{\times 2} \longrightarrow k(x)^\times/k(x)^{\times 2}$ induite par la norme $N_{M/k(x)} := \prod_{i=1}^{3} N_{K_i/k(x)}$. Par conséquent le polynôme $\prod_{i=1}^{r}\alpha_i$ est un carré dans $k(x)$.

Soient $i \in \{1, \cdots, r\}$ fixé et p un facteur premier de α_i. Puisque $\prod_{i=1}^{r}\alpha_i$ est un carré dans $k(x)$, sa valuation en p est paire. Or les α_j sont sans facteur carré, donc p doit diviser un nombre pair de α_j. De plus, p divise α_i donc p divise un nombre impair d'éléments de $\{\alpha_j \mid j \neq i\}$, ou de façon équivalente p divise un nombre impair de $\mu_{i,j} = \mathrm{pgcd}(\alpha_i, \alpha_j)$ (avec $j \neq i$). Le polynôme $\mu_{i,j}$ est sans facteur carré, donc de valuation 0 ou 1 en p. Par suite, $\Lambda_i = \Gamma_i^{-2}\prod_{j\neq i}\mu_{i,j}$ est de valuation impaire en p. Ainsi, tout facteur premier de α_i divise Λ_i. Or α_i est sans facteur carré, donc α_i divise Λ_i.

Réciproquement, nous montrons que Λ_i divise α_i. Soit p un facteur premier de Λ_i. Alors p divise $\mu_{i,j} = \mathrm{pgcd}(\alpha_i, \alpha_j)$ pour un certain $j \neq i$. En

particulier p est un diviseur de α_i. Ceci permet de conclure : puisque Λ_i est sans facteur carré, le polynôme Λ_i divise α_i.

Ainsi les polynômes α_i et Λ_i sont égaux à multiplication par un élément de $k^\times$ près. Par ailleurs, les polynômes Λ_i et α_i ont même coefficient dominant. Les deux polynômes α_i et Λ_i sont donc égaux, et par suite les classes de α_i et $\prod_{j\neq i} \mu_{i,j}$ dans $k(x)^\times/k(x)^{\times 2}$ sont égales.

D'après la proposition 3.3.1.3, les idéaux premiers de $\mathcal{O}_i$ en lesquels $\pi_{\mathcal{H},i}(\mathrm{Cl}(\mathrm{div}(u,v))$ a une valuation impaire sont des idéaux apparaissant dans la décomposition en idéaux premiers de la classe de $f'(y_i)$ dans K_i. Ainsi, les facteurs premiers de $\alpha_i \in k[x]$ sont des facteurs premiers de $N_{K_i/k(x)}(f'(y_i))$, c'est-à-dire des facteurs premiers de $N_{K_i/k(x)}(P_i'(y_i)\prod_{j\neq i} P_j(y_i))$ puisque

$$f'(T) \equiv P_i'(T)\prod_{j\neq i} P_j(T) \bmod P_i(T).$$

Les facteurs premiers de $\mu_{i,j} = \mathrm{pgcd}(\alpha_i, \alpha_j)$ sont donc des facteurs premiers de $d_{i,j} = \mathrm{pgcd}(N_{K_i/k(x)}(P_i'(y_i)\prod_{k\neq i} P_k(y_i)), N_{K_j/k(x)}(P_j'(y_j)\prod_{k\neq j} P_k(y_j)))$. □

Dans le cas particulier des courbes elliptiques, la proposition 4.1.3 est une conséquence de la proposition suivante (dont la démonstration est reprise de [CEP71]).

Proposition 4.1.4 *Soient k un corps de caractéristique 0 et K une extension de k. Soient S, $T \in k[x]$ tels que $T(S^2-4T) \neq 0$. Nous notons $\mathcal{D}$ la courbe elliptique d'équation de weierstrass*

$$\mathcal{D} : \beta^2 = \alpha(\alpha^2 + S\alpha + T).$$

Soit $(\alpha,\beta) \neq (0,0)$ un $K(x)$-point de $\mathcal{D}$.

Il existe alors $\epsilon \in K$, $\mu \in K[x]$ unitaire sans facteur carré divisant T et deux polynômes $\theta \in k[x]$ et $\psi \in k[x]$ tels que

* *$\mu\theta$ soit premier avec ψ,*
* *$\alpha = \epsilon\mu\frac{\theta^2}{\psi^2}$,*
* *$\epsilon\mu\nu^2 = \epsilon^2\mu^2\theta^4 + S\epsilon\mu\theta^2\psi^2 + T\psi^4$.*

Démonstration.

Nous commençons par écrire $\alpha = \frac{\chi}{\varphi}$ et $\beta = \frac{\xi}{\phi}$ avec χ, φ, ξ et $\phi \in K[x]$ des polynômes tels que

* χ et φ soient premiers entre eux,
* ξ et ϕ soient premiers entre eux, et
* ϕ et φ soient unitaires.

En chassant les dénominateurs dans l'équation de $\mathcal{D}$, nous obtenons :

$$\varphi^3\xi^2 = \phi^2\chi(\chi^2 + S\varphi\chi + T\varphi^2). \tag{4.1}$$

Comme ϕ^2 divise $\varphi^3\xi^2$ et est premier à ξ, le polynôme ϕ^2 divise φ^3. De même φ^3 divise $\phi^2\chi(\chi^2 + S\varphi\chi + T\varphi^2)$ et est premier à χ et à $(\chi^2 + S\varphi\chi + T\varphi^2)$ (car $\chi^2 + S\varphi\chi + T\varphi^2 \equiv \chi^2 \bmod \varphi$), donc φ^3 divise ϕ^2. Ainsi ϕ^2 et φ^3 sont égaux (ils sont tous deux unitaires). Il existe donc $\psi \in K[x]$ unitaire tel que $\varphi = \psi^2$ et $\phi = \psi^3$.

Nous posons $\chi = \epsilon\mu\theta^2$ avec $\epsilon \in K$ et μ, $\theta \in K[x]$ deux polynômes unitaires. L'équation 4.1 se réécrit alors

$$\xi^2 = \epsilon\mu\theta^2(\epsilon^2\mu^2\theta^4 + S\epsilon\mu\theta^2\psi^2 + T\psi^4).$$

Cette égalité impose à μ de diviser ξ et entraîne donc l'existence de $\nu \in K[x]$ tel que

$$\epsilon\mu\nu^2 = \epsilon^2\mu^2\theta^4 + S\epsilon\mu\theta^2\psi^2 + T\psi^4.$$

Cette égalité montre que μ divise $T\psi^4$. Par ailleurs μ est premier à ψ (puisqu'il divise χ). Le polynôme μ est donc un diviseur de T. □

Remarque :

Ce résultat étant plus précis que la proposition 4.1.3, nous l'utilisons au cours des sections 4.2 et 4.3. Ceci explique pourquoi nous ne parlons pas du morphisme $\Xi_{\mathcal{H}}$ au cours de ces deux sections.

Soient $\mathcal{P}$ une place de $k(x)$, $\mathcal{O}_{\mathcal{P}}$ l'anneau de valuation correspondant, et $k(\mathcal{P}) := \mathcal{O}_{\mathcal{P}}/\mathcal{P}$ le corps résiduel en $\mathcal{P}$. La surjection canonique $\mathcal{O}_{\mathcal{P}} \longrightarrow k(\mathcal{P})$ induit un morphisme $\mathrm{ev}_{\mathcal{P}} : \mathcal{O}_{\mathcal{P}}^{\times}/\mathcal{O}_{\mathcal{P}}^{\times 2} \longrightarrow k(\mathcal{P})^{\times}/k(\mathcal{P})^{\times 2}$.

La proposition 4.1.3 ne suffit en général pas à calculer $\mathrm{Im}(\Xi_{\mathcal{H}})$. Ainsi, comme dans [CEP71], nous devons affiner notre étude de $\mathrm{Im}(\Xi_{\mathcal{H}})$ en considérant la restriction de $\mathrm{ev}_{\mathcal{P}}$ à $\mathrm{Im}(\Xi_{\mathcal{H},i})$ et $\{p^{-1}\mu \mid \mu \in \mathrm{Im}(\Xi_{\mathcal{H},i})\}$ (avec p une uniformisante de $\mathcal{P}$). Ceci motive l'introduction de la notation suivante.

Notations 4.1.5 Soient $\mathcal{P}$ une place de $k(x)$ et $\mathcal{O}_{\mathcal{P}}$ l'anneau de valuation correspondant. Soit α, $\beta \in \mathcal{O}_{\mathcal{P}}^{\times}$.

Nous disons que α est équivalent à β modulo $\mathcal{P}$ et modulo les carrés, et nous notons $\alpha \sim \beta \bmod \mathcal{P}$, s'il existe $\gamma \in \mathcal{O}_{\mathcal{P}}^{\times}$ tel que α et $\beta\gamma^2$ soient dans la même classe modulo $\mathcal{P}$.

Dans ce qui suit, les places $\mathcal{P}$ pour lesquelles nous étudions le morphisme $\mathrm{ev}_{\mathcal{P}}$ sont soit la place à l'infini de $k(x)$, soit des places admettant un facteur premier du discriminant de f comme uniformisante. En effet, modulo les facteurs premiers de son discriminant, le polynôme $f(y)$ à un facteur carré. L'idée est d'utiliser l'existence d'un tel facteur carré pour comprendre $\mathrm{Im}(\Xi_{\mathcal{H}})$. À titre d'exemple, nous démontrons le résultat :

Proposition 4.1.6 *Soit k un corps de caractéristique 0. Soient $A \in k(x)$ et $K := k(x)[T]/(T^2 - A)$. Soit t la classe de T dans K.*

Soient $\mathcal{P}$ une place de $k(x)$, $\mathcal{O}_\mathcal{P}$ l'anneau de valuation correspondant et $v_\mathcal{P}$ la valuation associée. Soit p une uniformisante de $\mathcal{P}$. Nous conservons la notation 4.1.5. Nous supposons $v_\mathcal{P}(A)$ impaire.

Soit $u := u_0(y^2) + yu_1(y^2) \in k(x)[y]$ un polynôme. Nous notons $\alpha := p^{-v_\mathcal{P}(N_{K/k(x)}(u(t)))} N_{K/k(x)}(u(t)) \in \mathcal{O}_\mathcal{P}^\times$ et $\widetilde{A} := p^{-v_\mathcal{P}(A)} A \in \mathcal{O}_\mathcal{P}^\times$.

1. *Si $v_\mathcal{P}(N_{K/k(x)}(u(t)))$ est paire, alors $\alpha \sim 1 \bmod \mathcal{P}$;*
2. *si $v_\mathcal{P}(N_{K/k(x)}(u(t)))$ est impaire, alors $\alpha \sim -\widetilde{A} \bmod \mathcal{P}$ et*

$$\frac{v_\mathcal{P}(A)+1}{2} + v_\mathcal{P}(u_1(A)) \leq v_\mathcal{P}(u_0(A)).$$

Démonstration.

La valuation $v_\mathcal{P}((u_0(A))^2)$ est paire et la valuation $v_\mathcal{P}(A(u_1(A))^2)$ est impaire. Ces deux valuations sont donc différentes. Par suite, la valuation en $\mathcal{P}$ de $N_{K/k(x)}(u(t)) = (u_0(A))^2 - A(u_1(A))^2$ est $\mathrm{Min}(v_\mathcal{P}((u_0(A))^2), v_\mathcal{P}(A(u_1(A))^2))$.

Si $v_\mathcal{P}(N_{K/k(x)}(u(t)))$ est paire. Alors la valuation $v_\mathcal{P}(N_{K/k(x)}(u(t)))$ est égale à $v_\mathcal{P}((u_0(A))^2) = 2v_\mathcal{P}(u_0(A))$. En particulier, la valuation $v_\mathcal{P}((u_0(A))^2)$ est strictement inférieure à $v_\mathcal{P}(A(u_1(A))^2)$, et ainsi

$$p^{-v_\mathcal{P}(N_{K/k(x)}(u(t)))} A(u_1(A))^2 = p^{-v_\mathcal{P}((u_0(A))^2)} A(u_1(A))^2$$

est un élément de $\mathcal{P}$. Par suite, la classe de

$$\alpha = p^{-v_\mathcal{P}(N_{K/k(x)}(u(t)))}(u_0(A))^2 - p^{-v_\mathcal{P}(N_{K/k(x)}(u(t)))} A(u_1(A))^2$$

dans le corps résiduel en $\mathcal{P}$ est non nulle et égale à celle de

$$\begin{aligned} p^{-v_\mathcal{P}(N_{K/k(x)}(u(t)))}(u_0(A))^2 &= p^{-v_\mathcal{P}((u_0(A))^2)}(u_0(A))^2 \\ &= p^{-2v_\mathcal{P}(u_0(A))}(u_0(A))^2 \\ &= \left(p^{-v_\mathcal{P}(u_0(A))}(u_0(A))\right)^2. \end{aligned}$$

Si $v_\mathcal{P}(N_{K/k(x)}(u(t)))$ est impaire. Alors la valuation $v_\mathcal{P}(N_{K/k(x)}(u(t)))$ est égale à $v_\mathcal{P}(A(u_1(A))^2)$. En particulier, la valuation $v_\mathcal{P}((u_0(A))^2)$ est strictement supérieure à $v_\mathcal{P}(A(u_1(A))^2)$, et ainsi

$$p^{-v_\mathcal{P}(N_{K/k(x)}(u(t)))}(u_0(A))^2 = p^{-v_\mathcal{P}(A(u_1(A))^2)}(u_0(A))^2$$

est un élément de $\mathcal{P}$. Par suite, la classe de

$$\alpha = p^{-v_\mathcal{P}(N_{K/k(x)}(u(t)))}(u_0(A))^2 - p^{-v_\mathcal{P}(N_{K/k(x)}(u(t)))} A(u_1(A))^2$$

dans le corps résiduel en $\mathcal{P}$ est non nulle et égale à celle de

$$\begin{aligned} -p^{-v_{\mathcal{P}}(N_{K/k(x)}(u(t)))}A(u_1(A))^2 &= -p^{-v_{\mathcal{P}}(A(u_1(A))^2)}A(u_1(A))^2 \\ &= -\widetilde{A}(p^{-v_{\mathcal{P}}(u_1(A))}u_1(A))^2. \end{aligned}$$

De plus, la valuation $v_{\mathcal{P}}((u_0(A))^2)$ est supérieure ou égale à $v_{\mathcal{P}}(A(u_1(A))^2)+1$, donc

$$\frac{v_{\mathcal{P}}(A)+1}{2} + v_{\mathcal{P}}(u_1(A)) \leq v_{\mathcal{P}}(u_0(A)). \quad \square$$

Proposition 4.1.7 *Soit k un corps de caractéristique 0. Soient $A \in k(x)$ et $K := k(x)[T]/(T^2 - A)$.*

Soient $\mathcal{P}$ une place de $k(x)$, $\mathcal{O}_{\mathcal{P}}$ l'anneau de valuation correspondant et $v_{\mathcal{P}}$ la valuation associée. Soit p une uniformisante de $\mathcal{P}$. Nous conservons la notation 4.1.5.
Nous supposons que

* *la valuation $v_{\mathcal{P}}(A)$ est paire,*
* *$p^{-v_{\mathcal{P}}(A)}A$ n'est pas pas un carré dans le corps résiduel $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$.*

Alors, pour tout polynôme $u := u_0(y^2) + yu_1(y^2) \in k(x)[y]$, la valuation $v_{\mathcal{P}}(N_{K/k(x)}(u(t)))$ est paire.

Démonstration.

Nous supposons que la valuation $v_{\mathcal{P}}(N_{K/k(x)}(u(t)))$ est impaire. Nous notons $r := \mathrm{Min}\left(v_{\mathcal{P}}(u_0(A)), \frac{v_{\mathcal{P}}(A)}{2} + v_{\mathcal{P}}(u_1(A))\right)$. Lorsque les classes de deux éléments α et β de $\mathcal{O}_{\mathcal{P}}$ dans le corps résiduel $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$ sont égales, nous notons $\alpha \equiv \beta \bmod \mathcal{P}$.

Par définition de r, la valuation en $\mathcal{P}$ de

$$p^{-2r}N_{K/k(x)}(u(t)) = \left(p^{-r}u_0\left(A\right)\right)^2 - p^{-v_{\mathcal{P}}(A)}A\left(p^{(v_{\mathcal{P}}(A)/2-r)}u_1\left(A\right)\right)^2$$

est positive ou nulle. Cette valuation étant impaire elle est strictement positive, c'est-à-dire que

$$\left(p^{-r}u_0\left(A\right)\right)^2 \equiv p^{-v_{\mathcal{P}}(A)}A\left(p^{(v_{\mathcal{P}}(A)/2-r)}u_1\left(A\right)\right)^2 \bmod \mathcal{P}. \qquad (4.2)$$

Par définition de r, l'une des deux valuations $v_{\mathcal{P}}\left(p^{(v_{\mathcal{P}}(A)/2-r)}u_1\left(A\right)\right)$ et $v_{\mathcal{P}}\left(u_0\left(A\right)\right)$ est nulle. En fait, la congruence 4.2 impose à ces deux valuations d'être nulles. En particulier, l'élément $p^{-v_{\mathcal{P}}(A)}A$ appartenant à $\mathcal{O}_{\mathcal{P}}^{\times}$, la classe de $p^{(v_{\mathcal{P}}(A)/2-r)}u_1(A)$ dans le corps résiduel $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$ est inversible. Nous déduisons alors de la congruence 4.2 que

$$p^{-v_{\mathcal{P}}(A)}A \sim \left(\frac{p^{-r}u_0\left(A\right)}{p^{(v_{\mathcal{P}}(A)/2-r)}u_1\left(A\right)}\right)^2 \bmod \mathcal{P} \sim 1 \bmod \mathcal{P}.$$

Ceci contredit l'hypothèse selon laquelle $p^{-v_{\mathcal{P}}(A)}A$ n'est pas un carré dans le corps résiduel $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$. La valuation $v_{\mathcal{P}}(N_{K/k(x)}(u(t)))$ doit donc être paire. □

4.2 Étude des courbes $\mathcal{C}_{\delta}^{-}$.

Soit k un corps de caractéristique 0. Soient d, e, $\delta \in k[x]$ trois polynômes non nuls tels que $e^2 - 4d$ soit non nul. Dans cette section, nous étudions la courbe elliptique $\mathcal{E}$ d'équation de Weierstrass

$$\mathcal{E} : t^2 = s(s^2 - \delta(e^2 - 2d)s + (\delta d)^2)$$

Nous appliquons ensuite les résultats de l'étude aux cas particuliers où $\delta = \zeta$ et $\delta = \zeta x$ pour un certain $\zeta \in k$.

Nous calculons tout d'abord l'image de la torsion de $\mathcal{E}(k(x))$ par $\gamma_{\mathcal{E}}$.

Lemme 4.2.1 *Soit k un corps de caractéristique 0. Soient d, e, $\delta \in k(x)$ trois fractions rationnelles non nulles telles que $e^2 - 4d$ soit non nul.*

Alors le polynôme $s(s^2 - \delta(e^2 - 2d)s + \delta^2 d^2) \in k(x)[s]$ est sans facteur carré.

Démonstration.

Comme δd est non nul, les polynômes s et $s^2 - \delta(e^2 - 2d)s + \delta^2 d^2$ sont premier entre eux. De plus, le discriminant $\delta^2 e^2 \left(e^2 - 4d\right)$ du polynôme $s^2 - \delta(e^2 - 2d)s + \delta^2 d^2$ est non nul. Le polynôme $s^2 - \delta(e^2 - 2d)s + \delta^2 d^2$ est donc sans facteur carré. □

Proposition 4.2.2 *Soit k un corps de caractéristique 0. Soient d, e, $\delta \in k(x)$ trois fractions rationnelles non nulles telles que $e^2 - 4d$ soit non nul. Soit $\mathcal{E}$ la courbe elliptique sur $k(x)$ d'équation de Weierstrass*

$$\mathcal{E} : t^2 = s(s^2 - \delta(e^2 - 2d)s + \delta^2 d^2).$$

Nous supposons que d, $e^2 - 4d$ et $-\delta(e^2 - 4d)$ ne sont pas des carrés dans $k(x)$. Alors la torsion 2-primaire de $\mathcal{E}(k(x))$ est engendrée par les points de coordonnées

* *$(-\delta d, \Delta^3 de)$ si $-\delta = \Delta^2$ pour un certain $\Delta \in k(x)$,*
* *$(0, 0)$ si $-\delta$ n'est pas un carré dans $k(x)$.*

Démonstration.

Nous commençons par déterminer la 2-torsion de la courbe elliptique $\mathcal{E}$. Elle correspond aux points $(\alpha, 0)$ avec α une racine du polynôme $s(s^2 - \delta(e^2 - 2d)s + (\delta d)^2)$. Par hypothèse, $e^2 - 4d$ n'est pas un carré, donc le polynôme

$$g(s) := s^2 - \delta(e^2 - 2d)s + (\delta d)^2 = \left(s - \frac{\delta}{2}(e^2 - 2d)\right)^2 - \frac{1}{4}\delta^2 e^2(e^2 - 4d)$$

n'a pas de racine dans $k(x)$. Le polynôme $g(s)$ est donc irréductible (il est de degré 2). Par conséquent, la 2-torsion de $\mathcal{E}(k(x))$ est le groupe d'ordre 2 engendré par le point $(0,0)$.

Un point $P := (\alpha, \beta)$ de $\mathcal{E}(k(x))$ vérifie $2P = (0,0)$ si et seulement si la droite passant par $(0,0)$ et P est tangente à $\mathcal{E}$ en P.

Soit $\psi \in k(x)$. L'intersection de la droite $\{(y,z) \in k(x) \times k(x) \mid z = \psi y\}$ et de $\mathcal{E}(k(x))$ est l'ensemble des points $(y, \psi y) \in k(x) \times k(x)$ tels que y soit nul ou solution de l'équation

$$\psi^2 y = y^2 - \delta(e^2 - 2d)y + (\delta d)^2. \tag{4.3}$$

La droite d'équation $z = \psi y$ est donc tangente à la courbe $\mathcal{E}$ en un point autre que le point $(0,0)$ si et seulement si l'équation 4.3 admet une racine double, c'est-à-dire si le discriminant

$$(\delta(e^2 - 2d) + \psi^2)^2 - 4(\delta d)^2 = (\psi^2 + \delta e^2)(\psi^2 + \delta(e^2 - 4d))$$

de l'équation 4.3 est nul. Cela ne se produit que dans deux cas : lorsque $-\delta$ est carré dans $k(x)$, ou lorsque $-\delta(e^2 - 4d))$ est un carré dans $k(x)$. Comme $-\delta(e^2 - 4d)$ n'est pas un carré dans $k(x)$, le seul cas à étudier est celui où $-\delta \in k(x)^{\times 2}$.

Supposons qu'il existe $\Delta \in k(x)$ tel que $-\delta = \Delta^2$. L'équation 4.3 a une racine double lorsque que $\psi = \Delta e$ ou $\psi = -\Delta e$. Ces valeurs de ψ correspondent aux points $(-\delta d, \Delta^3 de)$ et $(-\delta d, -\Delta^3 de)$. Les points $(-\delta d, \Delta^3 de)$ et $(-\delta d, -\Delta^3 de)$ sont des points de 4-torsion.

Nous posons $K := k(x)[T]/(g(T))$ le corps de décomposition du polynôme $g(s)$. Soit $\pi_{\mathcal{E}} : \mathcal{E}(k(x)) \longrightarrow k(x)^\times / k(x)^{\times 2} \times K^\times / K^{\times 2}$ le morphisme de Cassels-Schaefer associé à $\mathcal{E}(k(x))$. Sa première coordonnée envoie un point (α, β) tel que α soit non nul sur la classe de α. Ainsi, comme d n'est pas un carré dans $k(x)$, les images par $\pi_{\mathcal{E}}$ de $(\Delta^2 d, \Delta^3 de)$ et de $(\Delta^2 d, -\Delta^3 de)$ ne sont pas triviales. Par conséquent, les points $(\Delta^2 d, \Delta^3 de)$ et de $(\Delta^2 d, -\Delta^3 de)$ ne sont pas des doubles dans $\mathcal{E}(k(x))$. □

Proposition 4.2.3 *Soit k un sous-corps de $\mathbb{R}$. Soient d, e, $\delta \in k[x]$ trois polynômes non nuls tels que $e^2 - 4d$ soit non nul. Soit $\mathcal{E}$ la courbe elliptique sur $k(x)$ d'équation de Weierstrass*

$$t^2 = s(s^2 - \delta(e^2 - 2d)s + \delta^2 d^2).$$

Nous conservons les notations 4.1 et 4.2. Nous supposons que d est unitaire de degré pair. Nous supposons de plus que $e^2 - 4d$ est de degré impair et que son coefficient dominant est strictement positif. Nous supposons enfin que le coefficient dominant ζ de δ est strictement positif.

Alors l'image de $\gamma_{\mathcal{E}}$ est contenue dans l'ensemble des classes dans $k(x)^\times / k(x)^{\times 2}$ de diviseurs unitaires sans facteur carré de δd de degré pair.

Démonstration.

Soit $P := (\alpha, \beta) \in \mathcal{E}(k(x))$. Le polynôme $e^2 - 4d \in k[x]$ n'est pas un carré dans $k(x)$ (il est de degré impair). Le polynôme $s^2 - \delta(e^2 - 2d)s + \delta^2 d^2$ est donc irréductible. Par suite, si $\beta = 0$, alors P est le point de coordonnées $(0, 0)$ (voir la démonstration de la proposition 4.2.2), et son image par $\gamma_{\mathcal{E}}$ est donc triviale.

Nous supposons que β est non nul. D'après la proposition 4.1.4, il existe $\epsilon \in k$, $\mu \in k[x]$ unitaire sans facteur carré divisant $(\delta d)^2$ et deux polynômes $\theta \in k[x]$ et $\psi \in k[x]$ tels que

* $\mu\theta$ soit premier avec ψ
* $\alpha = \epsilon\mu\frac{\theta^2}{\psi^2}$.

Nous appliquons la proposition 4.1.6 en prenant pour $\mathcal{P}$ la place à l'infini de $k(x)$, $A := \frac{\delta^2 e^2(e^2-4d)}{4}$ et $u(y) = y - \alpha + \frac{\delta(e^2-2d)}{2}$. Pour cela, nous notons $K_A := k(x)[y]/(y^2 - A)$ et y_A la classe de y dans K_A. Nous avons alors

$$\begin{aligned} N_{K_A/k(x)}(u(y_A)) &= N_{K_A/k(x)}\left(y_A - \alpha + \tfrac{\delta(e^2-2d)}{2}\right) \\ &= \left(\alpha - \tfrac{\delta(e^2-2d)}{2}\right)^2 - \tfrac{\delta^2 e^2(e^2-4d)}{4} \\ &= \alpha^2 - \delta(e^2 - 2d)\alpha + \delta^2 d^2. \end{aligned}$$

La valuation associée à la place à l'infini de $k(x)$ est $-\deg$. Ainsi, le lemme 4.1.6 affirme que la classe du coefficient dominant de $N_{K_A/k(x)}(u(y_A))$ dans $k^\times/k^{\times 2}$ est celle

* de 1 si $\deg(N_{K_A/k(x)}(u(y_A))) \equiv 0 \bmod 2$,
* du coefficient dominant de $4d-e^2$ si $\deg(N_{K_A/k(x)}(u(y_A))) \equiv 1 \bmod 2$.

Soit λ le coefficient de $e^2 - 4d$.

Le point P est un point de $\mathcal{E}(k(x))$, donc $\beta^2 = \alpha N_{K_A/k(x)}(u(y_A))$. Les fractions rationnelles α et $N_{K_A/k(x)}(u(y_A))$ sont donc non nulles (car $\beta \neq 0$). Ainsi, puisque $\alpha \sim \epsilon\mu$, nous avons $\epsilon\mu \sim N_{K_A/k(x)}(u(y_A))$. Le polynôme μ étant unitaire, nous déduisons de cette équivalence que

* $\epsilon \sim 1$ si $\deg(\alpha) \equiv 0 \bmod 2$,
* $\epsilon \sim -\lambda$ si $\deg(\alpha) \equiv 1 \bmod 2$.

Nous supposons maintenant que $\deg(\alpha) \equiv 1 \bmod 2$, c'est-à-dire que $\deg(N_{K_A/k(x)}(u(y_A))) \equiv 1 \bmod 2$. Alors, d'après le lemme 4.1.6, nous avons

$$\deg\left(\alpha - \frac{\delta(e^2 - 2d)}{2}\right) \leq \frac{-1 + \deg(\delta^2 e^2(e^2 - 4d))}{2}. \tag{4.4}$$

Bien que $\deg(e^2)$ et $\deg(d)$ soient pairs, le degré $\deg(e^2 - 4d)$ est impair. Nous avons donc $\deg(e^2) = \deg(d) > \deg(e^2 - 4d)$. Par suite, le degré de $e^2 - 2d = \frac{e^2-4d}{2} + \frac{e^2}{2}$ est $\deg(e^2)$. Nous en déduisons que

$$\begin{aligned} 2\deg(e^2 - 2d) &= 2\deg(e^2) \\ &> \deg(e^2) + \deg(e^2 - 4d) = \deg(e^2(e^2 - 4d)). \end{aligned}$$

En ajoutant $2\deg(\delta)$ aux deux membres de cette inégalité, nous montrons

$$\begin{array}{rcl} 2\deg\left(\delta\left(e^2-2d\right)\right) & > & \deg(\delta^2e^2(e^2-4d)) \\ & > & -1+\deg(\delta^2e^2(e^2-4d)). \end{array} \tag{4.5}$$

L'inégalité 4.5 ne peut être cohérente avec l'inégalité 4.4 que dans le cas où $\alpha\psi^2$ (c'est-à-dire $\epsilon\mu\theta^2$) et $\frac{\delta(e^2-2d)}{2}\psi^2$ ont même degré et même coefficient dominant.

Comme $\deg(d) > \deg(e^2-4d)$ et d est unitaire, le coefficient dominant de $e^2-2d = \left(e^2-4d\right)+2d$ est 2. Le polynôme μ étant unitaire, nous venons de montrer que $\epsilon \sim \zeta$. Or $\epsilon \sim -\lambda$, donc $-\zeta\lambda$ est un carré dans k. Ce n'est pas possible : k est un sous-corps de $\mathbb{R}$ et $\zeta\lambda > 0$. Par suite le degré $\deg(\alpha)$ est toujours pair. $\square$

Proposition 4.2.4 *Soit k un corps de caractéristique 0. Soient d, e, $\delta \in k[x]$ trois polynômes non nuls tels que e^2-4d soit non nul. Soit $\mathcal{E}$ la courbe elliptique sur $k(x)$ d'équation de Weierstrass*

$$t^2 = s(s^2-\delta(e^2-2d)s+\delta^2d^2).$$

Nous conservons les notations 4.2 et 4.1.

Soit p un facteur premier de e qui ne divise pas δd. Nous supposons que le polynôme $e^2-4d \in k[x]$ est de degré impair.

Alors l'image de $\gamma_{\mathcal{E}}$ est contenue dans l'ensemble des classes dans $k(x)^\times/k(x)^{\times 2}$ de diviseurs μ sans facteur carré de δd tels que

$$\mu \sim 1 \bmod p \text{ ou } \mu \sim -\delta d \bmod p.$$

Démonstration.

Soit $P := (\alpha,\beta) \in \mathcal{E}(k(x))$. Le polynôme $e^2-4d \in k[x]$ n'est pas un carré dans $k(x)$ (il est de degré impair). Le polynôme $s^2-\delta(e^2-2d)s+\delta^2d^2$ est donc irréductible. Par suite, si $\beta = 0$, alors P est le point de coordonnées $(0,0)$ (voir la démonstration de la proposition 4.2.2), et son image par $\gamma_{\mathcal{E}}$ est donc triviale.

Nous supposons que β est non nul. D'après la proposition 4.1.4, il existe $\mu \in k[x]$ sans facteur carré divisant $(\delta d)^2$ et deux polynômes $\theta \in k[x]$ et $\psi \in k[x]$ tels que

* $\mu\theta$ soit premier avec ψ
* $\alpha = \mu\frac{\theta^2}{\psi^2}$
* $\mu\nu^2 = \mu^2\theta^4 - \delta(e^2-2d)\mu\theta^2\psi^2 + (\delta d)^2\psi^4$.

Puisque p est un facteur premier de e, nous avons la congruence

$$\mu\nu^2 \equiv (\mu\theta^2+\delta d\psi^2)^2 \bmod p. \tag{4.6}$$

Lorsque ν est inversible modulo p, nous déduisons de la congruence 4.6 que $\mu \sim 1 \bmod p$.

Supposons que p divise ν. D'après la congruence 4.6, nous avons

$$\mu\theta^2 \equiv -\delta d\psi^2 \bmod p.$$

Comme δd et μ sont premiers à p, nous savons que θ est divisible par p si et seulement si ψ est divisible par p. Or les polynômes θ et ψ sont premiers entre eux, donc p ne divise ni θ ni ψ. Nous déduisons alors de la congruence $\mu\theta^2 \equiv -\delta d\psi^2 \bmod p$ que $\mu \sim -\delta d \bmod p$. □

Proposition 4.2.5 *Soient η, ω, $\rho \in \mathbb{R}$ des réels. Soit $k := \mathbb{Q}(\eta, \omega, \rho)$. Nous posons :*

$$b_1 = \frac{\rho^2 - \eta^2}{\omega^2 - \eta^2} + \frac{\eta^2 - \omega^2}{4}.$$

Soient $B(x) := (x + b_1)^2 - \eta^2$ et $C(x) := 2(x + b_1) + \omega^2 - \eta^2 - 1$.

À tout $\zeta \in k^\times$, nous associons la $k(x)$-courbe elliptique $\mathcal{C}_\zeta^-$ d'équation affine :

$$\mathcal{C}_\zeta^- : t^2 = s\left(s^2 - \zeta\left((1-C)^2 - 2\left(B-C\right)\right)s + \zeta^2\left(B-C\right)^2\right).$$

Nous conservons les notations 4.2 et 4.1. Nous supposons que

* *$\omega^2 > \eta^2$, et*
* *$\left(\omega^2 - \eta^2\right)^2 - 4\omega^2 = \left(\omega^2 - \eta^2 - 2\omega\right)\left(\omega^2 - \eta^2 + 2\omega\right)$ n'est pas un carré dans k.*

Alors, pour tout $\zeta \in k$ strictement positif, l'image de $\gamma_{\mathcal{C}_\zeta^-, k(x)}$ est triviale.

Démonstration.

Soit $\zeta \in k$ strictement positif. Nous appliquons les propositions 4.2.3 et 4.2.4 avec $e = 1 - C$, $d = B - C$ et $\delta = \zeta$.

Le polynôme $e = 1 - C$ est de degré 1. Il est donc non nul. De même, comme $\deg(B - C) = 2$, le polynôme $d = B - C$ est non nul.

Le polynôme $e^2 - 4d = (1 - C)^2 - 4(B - C) = 4\left(\omega^2 - \eta^2\right)x + 4\rho^2$ est de degré 1 (car $\omega^2 > \eta^2$). En particulier, le polynôme $e^2 - 4d$ est non nul. Ainsi, puisque $\delta = \zeta \in k^\times$, le polynôme

$$s(s^2 - \zeta((1-C)^2 - 2(B-C))s + \zeta^2(B-C)^2)$$

est sans facteur carré (voir le lemme 4.2.1).

Le polynôme $e^2 - 4d = (1 - C)^2 - 4(B - C)$ est de degré impair et son coefficient dominant (qui vaut $4\left(\omega^2 - \eta^2\right)$) est strictement positif par hypothèse.

De plus, le polynôme $d = B - C$ est unitaire de degré 2. Ainsi, comme ζ est strictement positif, les hypothèses de la proposition 4.2.3 sont satisfaites.

Par conséquent, l'image de $\gamma_{\mathcal{C}_\zeta^-}$ est contenue dans l'ensemble des classes dans $k(x)^\times/k(x)^{\times 2}$ de diviseurs μ unitaires de degré pair de $B-C$. Soit μ un tel diviseur. Le polynôme $B-C$ étant unitaire de degré 2, nous avons deux possibilités :

$$\mu \sim 1 \text{ ou } \mu \sim (B-C).$$

Le reste de la division euclidienne de $\delta d = \zeta(B-C) = \zeta[(x+b_1-1)^2-\omega^2]$ par $e = 1-C = \eta^2-\omega^2-2(x+b_1-1)$ est

$$\frac{\left(\omega^2-\eta^2\right)^2-4\omega^2}{4} = \frac{1}{4}(\omega^2-\eta^2+2\omega)(\omega^2-\eta^2-2\omega).$$

Ce n'est pas un carré dans k. En particulier, ce reste n'est pas nul. Ainsi, puisque le polynôme $e^2-4d \in k[x]$ est de degré 1, les hypothèses de la proposition 4.2.4 sont vérifiées. Cette proposition affirme que

$$\mu \sim 1 \bmod (1-C) \text{ ou } \mu \sim -\zeta(B-C) \bmod (1-C).$$

Lorsque $\mu \sim (B-C)$, nous avons

$$B-C \sim 1 \bmod (1-C) \text{ ou } B-C \sim -\zeta(B-C) \bmod (1-C).$$

La première alternative signifie que le reste $\left(\omega^2-\eta^2\right)^2-4\omega^2$ de la division euclidienne de $4(B-C)$ par $1-C$ est un carré dans k, ce qui est exclu.

La deuxième alternative est également impossible car $-\zeta$ n'est pas un carré dans k (k est un sous-corps de $\mathbb{R}$ et l'élément $-\zeta$ est strictement négatif). Le cas $\mu \sim (B-C)$ est donc impossible. □

Les propositions 4.2.3 et 4.2.4 nous permettent de traiter complètement le cas où δ est un élément strictement positif de k. Elle sont cependant insuffisantes dans le cas où δ est un multiple de x.

Proposition 4.2.6 *Soit k un corps de caractéristique 0. Soient d, e, $\delta \in k[x]$ trois polynômes non nuls tels que e^2-4d soit non nul. Soit $\mathcal{E}$ la courbe elliptique sur $k(x)$ d'équation de Weierstrass*

$$t^2 = s(s^2-\delta(e^2-2d)s+\delta^2d^2).$$

Nous conservons les notations 4.2 et 4.1.

Soit p un facteur premier de δ. Nous supposons que $v_p(\delta) = 1$ et $v_p(d) = v_p(e) = 0$. Nous supposons aussi que le polynôme $e^2-4d \in k[x]$ est de degré impair.

Alors l'image de $\gamma_{\mathcal{E}}$ est contenue dans l'ensemble des classes dans $k(x)^\times/k(x)^{\times 2}$ de diviseurs sans facteur carré μ de δd tels que

* *$\mu \sim 1 \bmod p$ si $v_p(\mu) = 0$, et*
* *$p^{-1}\mu \sim p^{-1}\delta \bmod p$ si $v_p(\mu) = 1$.*

Démonstration.

Soit $P := (\alpha, \beta) \in \mathcal{E}(k(x))$. Le polynôme $e^2 - 4d \in k[x]$ n'est pas un carré dans $k(x)$ (il est de degré impair). Le polynôme $s^2 - \delta(e^2 - 2d)s + \delta^2 d^2$ est donc irréductible. Par suite, si $\beta = 0$, alors P est le point de coordonnées $(0, 0)$ (voir la démonstration de la proposition 4.2.2), et son image par $\gamma_{\mathcal{E}}$ est donc triviale.

Nous supposons que β est non nul (le cas où P est un point de ramification est direct). D'après la proposition 4.1.4, il existe $\mu \in k[x]$ sans facteur carré divisant $(\delta d)^2$ et deux polynômes $\theta \in k[x]$ et $\psi \in k[x]$ tels que

* $\mu\theta$ soit premier avec ψ
* $\alpha = \mu\frac{\theta^2}{\psi^2}$.

La proposition 4.1.4 affirme également que

$$\mu\nu^2 = \mu^2\theta^4 - \delta(e^2 - 2d)\mu\theta^2\psi^2 + (\delta d)^2\psi^4. \tag{4.7}$$

Le cas où $v_p(\mu) = 0$. Nous réduisons l'équation 4.7 modulo p. Puisque p divise δ, nous avons

$$\mu\nu^2 \equiv \mu^2\theta^4 \bmod p.$$

Si θ est premier à p, alors $\mu \equiv (\nu\theta^{-2})^2 \bmod p$ et donc μ est un carré non nul modulo p.

Nous supposons maintenant que p divise θ. Le polynôme p étant un facteur premier de δ, il divise $\mu\theta^2 + \delta(e^2 - 4d)\psi^2$ et donc

$$\begin{array}{rcl} v_p(\mu\theta^2(\mu\theta^2 + \delta(e^2 - 4d)\psi^2)) & \geq & 2v_p(\theta) + v_p(\mu\theta^2 + \delta(e^2 - 4d)\psi^2) \\ & \geq & 2 + 1 = 3. \end{array}$$

Nous exprimons cette valuation en utilisant l'égalité

$$\mu\theta^2(\mu\theta^2 + \delta(e^2 - 4d)\psi^2) = \mu\nu^2 - \delta^2 d^2\psi^4$$

(qui est une reformulation de l'équation 4.7). Les polynômes ψ et θ sont premiers entre eux. Le polynôme ψ est donc premier à p. Par suite, la valuation $v_p(\delta^2 d^2\psi^4)$ est égale à 2. Or $v_p(\mu\nu^2 - \delta^2 d^2\psi^4) \geq 3 > 2$, donc la valuation $v_p(\mu\nu^2)$ est égale à 2. Nous pouvons maintenant conclure :

$$\begin{array}{rcl} \mu(\nu p^{-1})^2 & = & p\left(p\mu^2(p^{-1}\theta)^4 - (p^{-1}\delta)(e^2 - 2d)\mu(p^{-1}\theta)^2\psi^2\right) + (p^{-1}\delta d)^2\psi^4 \\ & \equiv & (\delta p^{-1})^2 d^2\psi^4 \bmod p \end{array}$$

et νp^{-1} est premier à p, donc $\mu \sim 1 \bmod p$.

Le cas où $v_p(\mu) = 1$. Soient $\widetilde{\mu} \in k[x]$ et $\widetilde{\delta} \in k[x]$ deux polynômes tels que $\mu = p\widetilde{\mu}$ et $\delta = p\widetilde{\delta}$. Après simplifications, l'équation 4.7 devient

$$\widetilde{\mu}\nu^2 = p\left(\widetilde{\mu}^2\theta^4 - \widetilde{\delta}(e^2 - 2d)\widetilde{\mu}\theta^2\psi^2 + (\widetilde{\delta}d)^2\psi^4\right).$$

En particulier, le polynôme p divise $\widetilde{\mu}\nu^2$. Or p est premier à $\widetilde{\mu}$ (car μ est sans facteur carré), donc p divise ν. Soit $\widetilde{\nu} \in k[x]$ un polynôme tel que $\nu = p\widetilde{\nu}$. L'équation 4.7 se réécrit

$$p\widetilde{\mu}\widetilde{\nu}^2 = \widetilde{\mu}^2\theta^4 - \widetilde{\delta}(e^2 - 2d)\widetilde{\mu}\theta^2\psi^2 + (\widetilde{\delta}d)^2\psi^4$$

c'est-à-dire

$$p\widetilde{\mu}\widetilde{\nu}^2 = \left(\widetilde{\mu}\theta^2 + \widetilde{\delta}d\psi^2\right)^2 - \widetilde{\delta}e^2\widetilde{\mu}\theta^2\psi^2.$$

Nous avons en particulier la congruence

$$\widetilde{\delta}e^2\widetilde{\mu}\theta^2\psi^2 \equiv \left(\widetilde{\mu}\theta^2 + \widetilde{\delta}d\psi^2\right)^2 \bmod p. \tag{4.8}$$

Supposons que p divise θ. Alors, d'après la congruence 4.8, le polynôme p divise $\widetilde{\delta}d\psi^2$. Le polynôme ψ est premier à θ, donc p est premier à ψ. De plus, $v_p(\delta d) = 1$ donc p ne divise pas $\widetilde{\delta}d\psi^2$. Par conséquent, le polynôme p ne divise pas θ.

Supposons que p divise ψ. Alors p divise $\widetilde{\mu}\theta^2$ (d'après la congruence 4.8). Comme θ et ψ sont premier entre eux, θ n'est pas divisible par p. De plus, μ est sans facteur carré, donc p ne divise pas $\widetilde{\mu}$. Finalement, p ne divise pas $\widetilde{\mu}\theta^2$. Par conséquent, le polynôme p ne divise pas ψ.

Puisque e, θ et ψ sont premiers à p, nous déduisons de la congruence 4.8 que $\widetilde{\mu} \sim \widetilde{\delta} \bmod p$. □

Proposition 4.2.7 *Soient η, ω, $\rho \in \mathbb{R}$ des réels. Soit $k := \mathbb{Q}(\eta, \omega, \rho)$. Nous posons :*

$$b_1 = \frac{\rho^2 - \eta^2}{\omega^2 - \eta^2} + \frac{\eta^2 - \omega^2}{4}.$$

Soient $B(x) := (x + b_1)^2 - \eta^2$ et $C(x) := 2(x + b_1) + \omega^2 - \eta^2 - 1$.

À tout $\zeta \in k^\times$, nous associons la $k(x)$-courbe elliptique $\mathcal{C}^-_{\zeta x}$ d'équation affine :

$$\mathcal{C}^-_{\zeta x} : t^2 = s\left(s^2 - \zeta x\left((1 - C)^2 - 2\,(B - C)\right)s + \zeta^2 x^2\,(B - C)^2\right).$$

Nous conservons les notations 4.2 et 4.1. Nous supposons que $\omega^2 > \eta^2$ et que les éléments

- $(b_1 - 1 + \omega)(b_1 - 1 - \omega)$,
- $(2b_1 - 2 + \omega^2 - \eta^2)(\omega^2 - \eta^2 + 2\omega)$,
- $(2b_1 - 2 + \omega^2 - \eta^2)(\omega^2 - \eta^2 - 2\omega)$,
- $2(\omega^2 - \eta^2 - 2\omega)(b_1 - 1 - \omega)$, *et*
- $2(\omega^2 - \eta^2 + 2\omega)(b_1 - 1 + \omega)$

ne sont pas des carrés dans k.

Alors, pour tout $\zeta \in k$ strictement positif, l'image de $\gamma_{\mathcal{C}^-_{\zeta x}, k(x)}$ est triviale.

Démonstration.

Soit $\zeta \in k$ strictement positif. Nous appliquons les propositions 4.2.3, 4.2.4 et 4.2.6 avec $e = 1 - C$, $d = B - C$ et $\delta = \zeta x$.

Le polynôme $e = 1 - C$ est de degré 1. Il est donc non nul. De même, comme $\deg(B - C) = 2$, le polynôme $d = B - C$ est non nul.

Le polynôme $e^2 - 4d = (1 - C)^2 - 4(B - C) = 4\left(\omega^2 - \eta^2\right) x + 4\rho^2$ est de degré 1 (car $\omega^2 > \eta^2$). En particulier, le polynôme $e^2 - 4d$ est non nul. Ainsi, puisque $\delta = \zeta x$ est non nul, le polynôme

$$s(s^2 - \zeta((1 - C)^2 - 2(B - C))s + \zeta^2(B - C)^2)$$

est sans facteur carré (voir le lemme 4.2.1).

Le polynôme $e^2 - 4d = (1 - C)^2 - 4(B - C)$ est de degré 1 et son coefficient dominant (qui vaut $\omega^2 - \eta^2$) est strictement positif par hypothèse. De plus, le polynôme $d = B - C$ est unitaire de degré 2. Enfin, ζ est strictement positif. Nous sommes donc sous les hypothèses de la proposition 4.2.3. Par conséquent, l'image de $\gamma_{\mathcal{C}_\zeta^-}$ est contenue dans l'ensemble des classes de diviseurs μ unitaires de degré pair de $\delta d = \zeta x(B - C)$. Soit μ un tel diviseur. Comme $B - C = (x + b_1 - 1)^2 - \omega^2$, nous avons quatre valeurs possibles pour μ :

1. $\mu = 1$,
2. $\mu = x(x + b_1 - 1 - \omega)$,
3. $\mu = x(x + b_1 - 1 + \omega)$, ou
4. $\mu = (B - C)$

L'élément $d(0) = B(0) - C(0) = (b_1 - 1)^2 - \omega^2$ n'est pas un carré dans k. Il n'est donc pas nul. De plus, $e(0) = 1 - C(0) = -\left(2b_1 - 2 + \omega^2 - \eta^2\right)$ est non nul (car $(2b_1 - 2 + \omega^2 - \eta^2)(\omega^2 - \eta^2 + 2\omega)$ n'est pas un carré dans k). Le polynôme $\delta = \zeta x$ est donc premier au polynôme ed. Les hypothèses de la proposition 4.2.6 (avec $\delta = \zeta x$) sont donc satisfaites.

Le cas où $\mu = (B - C)$. D'après la proposition 4.2.6, nous avons $\mu \sim 1 \bmod x$, c'est-à-dire $B(0) - C(0) = (b_1 - 1)^2 - \omega^2 \in k^{\times 2}$. Nous avons une contradiction avec les hypothèses. Le cas $\mu = B - C$ est donc impossible.

Le cas où $\mu = x(x + b_1 - 1 - \omega)$. D'après la proposition 4.2.6, nous avons $x + b_1 - 1 - \omega \sim \zeta \bmod x$, c'est-à-dire

$$b_1 - 1 - \omega \sim \zeta.$$

Le reste de la division euclidienne par $1 - C = -2(x + b_1 - 1) + \eta^2 - \omega^2$

* de x est $-\frac{2b_1-2+\omega^2-\eta^2}{2}$,
* de $B-C=(x+b_1-1)^2-\omega^2$ est $\left(\frac{\omega^2-\eta^2}{2}\right)^2-\omega^2=\frac{(\omega^2-\eta^2+2\omega)(\omega^2-\eta^2-2\omega)}{4}$.

Ces deux restes sont non nuls (les éléments $(2b_1-2+\omega^2-\eta^2)(\omega^2-\eta^2+2\omega)$ et $(2b_1-2+\omega^2-\eta^2)(\omega^2-\eta^2-2\omega)$ ne sont pas des carrés dans k). Les hypothèses de la proposition 4.2.4 sont donc satisfaites.

D'après la proposition 4.2.4, nous avons

$$\mu \sim 1 \bmod (1-C) \text{ ou } \mu \sim -\zeta x(B-C) \bmod (1-C),$$

c'est-à-dire

$$x(x+b_1-1-\omega) \sim 1 \bmod (1-C) \text{ ou } -\zeta \sim (x+b_1-1+\omega) \bmod (1-C).$$

Étant donné que $1-C=-2(x+b_1-1)+\eta^2-\omega^2$, cela signifie que

$$(2b_1-2+\omega^2-\eta^2)(\omega^2-\eta^2+2\omega) \sim 1 \text{ ou } \zeta \sim 2(\omega^2-\eta^2-2\omega).$$

Le premier cas est exclu par hypothèse. Dans le second cas, nous avons

$$\zeta \sim 2(\omega^2-\eta^2-2\omega) \text{ et } \zeta \sim (b_1-1-\omega).$$

Le second cas est également exclu car $2(\omega^2-\eta^2-2\omega)(b_1-1-\omega) \notin k^{\times 2}$. Finalement, μ ne peut être égal à $x(x+b_1-1-\omega)$.

Le cas où $\mu = x(x+b_1-1+\omega)$. Par symétrie des rôles de ω et $-\omega$, ce cas n'est pas possible. □

4.3 Etude de la courbe $\widehat{\mathcal{C}_\delta^-}$.

Soit k un corps de caractéristique 0. Soient d, e, $\delta \in k[x]$ trois polynômes non nuls tels que e^2-4d soit non nul. Dans cette section, nous étudions la courbe elliptique $\mathcal{E}$ d'équation de Weierstrass

$$\mathcal{E} : t^2 = s(s+\delta e^2)(s+\delta(e^2-4d)).$$

Nous appliquons ensuite les résultats de l'étude aux cas particuliers où $\delta=\zeta$ et $\delta=\zeta x$ pour un certain $\zeta \in k$.

Proposition 4.3.1 *Soit k un corps de caractéristique 0. Soient d, e, $\delta \in k[x]$ trois polynômes non nuls tels que e^2-4d soit non nul.*

Soit $\mathcal{E}$ la courbe elliptique sur $k(x)$ d'équation de Weierstrass

$$\mathcal{E} : t^2 = s(s+\delta e^2)(s+\delta(e^2-4d)).$$

Nous supposons que les polynômes e^2-4d, $-\delta$ et $-\delta(e^2-4d)$ ne sont pas des carrés dans $k(x)$.

Nous conservons les notations 4.2 et 4.1.

Alors la torsion 2-primaire de $\mathcal{E}(k(x))$ est engendrée par $(-\delta,0)$ et $(e^2-4d,0)$. En particulier, l'image par $\gamma_{\mathcal{E}}$ de la torsion de $\mathcal{E}(k(x))$ est engendrée par les classes $\left[e^2-4d\right]$ et $[-\delta]$.

Démonstration.

Comme les polynômes δ, e, $e^2 - 4d$ et d sont non nuls, le polynôme $s(s + \delta e^2)(s + \delta(e^2 - 4d))$ (à coefficients dans $k(x)$) est sans facteur carré.

La courbe $\mathcal{E}$ possède trois points de 2-torsion : les points de coordonnées $(0, 0)$, $(-\delta e^2, 0)$ et $(-\delta(e^2 - 4d), 0)$.

Les éléments $-\delta$, $e^2 - 4d$ et $-\delta(e^2 - 4d)$ ne sont pas des carrés dans $k(x)$, donc les les images

* $\gamma_{\mathcal{E}}\left(-\delta e^2, 0\right) = [-\delta]$,
* $\gamma_{\mathcal{E}}\left(-\delta\left(e^2 - 4d\right), 0\right) = \left[-\delta\left(e^2 - 4d\right)\right]$ et
* $\gamma_{\mathcal{E}}\left(0, 0\right) = \gamma_{\mathcal{E}}\left(-\delta e^2, 0\right) + \gamma_{\mathcal{E}}\left(-\delta\left(e^2 - 4d\right), 0\right) = \left[e^2 - 4d\right]$

ne sont pas triviales (l'image $\gamma_{\mathcal{E}}\left(0, 0\right)$ est calculée en remarquant que $(0, 0) = \left(-\delta e^2, 0\right) + \left(-\delta\left(e^2 - 4d\right), 0\right)$).

Or les éléments de $2\mathcal{E}(k(x))$ sont d'image triviale par $\gamma_{\mathcal{E}}$, donc les points de coordonnées $\left(0, 0\right)$, $\left(-\delta e^2, 0\right)$ et $\left(-\delta\left(e^2 - 4d\right), 0\right)$ ne sont donc pas des doubles dans $\mathcal{E}(k(x))$.

Comme l'image d'un double par $\gamma_{\mathcal{E}}$ est triviale, nous avons, pour tout entier $m \in \mathbb{N}$ impair, l'égalité $\gamma_{\mathcal{E}}(T) = \gamma_{\mathcal{E}}(mT)$. En particulier, pour tout $m \in \mathbb{N}$ impair, tout $n \in \mathbb{N}$ et tout point de $(2^n m)$-torsion T, l'image $\gamma_{\mathcal{E}}(T)$ est l'image du point de 2^n-torsion mT par $\gamma_{\mathcal{E}}$. Ainsi, l'image de la torsion de $\mathcal{E}(k(x))$ par $\gamma_{\mathcal{E}}$ est l'image de la torsion 2-primaire de $\mathcal{E}(k(x))$, c'est-à-dire l'image de la 2-torsion de $\mathcal{E}(k(x))$. □

Proposition 4.3.2 *Soit k un corps de caractéristique 0. Soient d, e, $\delta \in k[x]$ trois polynômes non nuls tels que $e^2 - 4d$ soit non nul.*

Soit $\mathcal{E}$ la courbe elliptique sur $k(x)$ d'équation de Weierstrass

$$\mathcal{E} : t^2 = s(s + \delta e^2)(s + \delta(e^2 - 4d)).$$

Nous conservons les notations 4.2 et 4.1.

Nous supposons que e est sans facteur carré. Nous supposons de plus qu'il n'existe aucun facteur premier p de e tel que $-\delta d$ soit un carré (éventuellement nul) modulo p.

Alors l'image de $\gamma_{\mathcal{E}}$ est contenue dans l'ensemble des classes dans $k(x)^\times / k(x)^{\times 2}$ de diviseurs de $\delta(e^2 - 4d)$.

Démonstration.

Puisque les polynômes δ, e, d et $e^2 - 4d$ sont non nuls, le polynôme $s(s + \delta e^2)(s + \delta(e^2 - 4d))$ (à coefficients dans $k(x)$) est sans facteur carré.

Soit $P := (\alpha, \beta)$ un $k(x)$-point de $\mathcal{E}$. Nous supposons que β est non nul (le cas où $\beta = 0$ est direct).

D'après la proposition 4.1.4, il existe une constante $\epsilon \in k^\times$, un polynôme $\mu \in k[x]$ unitaire sans facteur carré divisant $\delta^2 e^2 (e^2 - 4d)$ et deux polynômes $\theta \in k[x]$ et $\psi \in k[x]$ tels que

* $\mu\theta$ soit premier avec ψ.
* $\alpha = \epsilon\mu\frac{\theta^2}{\psi^2}$.

La proposition 4.1.4 affirme également que

$$\epsilon\mu\nu^2 \quad = \quad (\epsilon\mu\theta^2 + \delta e^2\psi^2)(\epsilon\mu\theta^2 + \delta(e^2 - 4d)\psi^2). \tag{4.9}$$

Supposons que e et $\delta(e^2 - 4d)$ aient un facteur commun p. Nous avons alors

$$\begin{aligned} -\delta d &\equiv \tfrac{\delta}{4}(e^2 - 4d) \bmod p \\ &\equiv 0 \bmod p. \end{aligned}$$

En particulier, $-\delta d$ est un carré modulo p, ce qui contredit les hypothèses. Les polynômes e et $\delta(e^2 - 4d)$ sont donc premiers entre eux. Soient

* $\mu_1 := \mathrm{pgcd}(\mu, \delta(e^2 - 4d))$,
* $e_1 := \mathrm{pgcd}(\mu, e)$,
* $e_2 \in k[x]$ l'unique polynôme tel que $e = e_1 e_2$, et
* $\mu_2 \in k[x]$ l'unique polynôme tel que $\delta(e^2 - 4d) = \mu_1\mu_2$.

Le polynôme μ est sans facteur carré et les polynômes e et $\delta(e^2 - 4d)$ sont premiers entre eux, donc $\mu = \mu_1 e_1$. Ainsi, après simplifications, l'équation 4.9 s'écrit :

$$\epsilon\nu^2 \quad = \quad (\epsilon\mu_1\theta^2 + \delta e_1 e_2^2\psi^2)(\epsilon e_1\theta^2 + \mu_2\psi^2). \tag{4.10}$$

Nous supposons maintenant que μ et e ont un facteur premier commun p. Alors e_1 est divisible par p. Ainsi, en réduisant l'équation 4.10 modulo p, nous obtenons la congruence

$$\begin{aligned} \epsilon\nu^2 &\equiv \epsilon\mu_1\mu_2\theta^2\psi^2 \bmod p \\ &\equiv \epsilon\delta(e^2 - 4d)\theta^2\psi^2 \bmod p \\ &\equiv -4\epsilon\delta d\theta^2\psi^2 \bmod p. \end{aligned} \tag{4.11}$$

Si p divise θ : D'après la congruence 4.11, p divise ν. En fait, p^2 divise ν^2, $\mu\theta^4$, $\delta e^2\theta^2\psi^2$ et $\delta(e^2 - 4d)\theta^2\psi^2$. Nous en déduisons que le polynôme

$$\delta e_1 e_2^2\mu_2\psi^4 = \epsilon\nu^2 - \epsilon^2\mu\theta^4 - \epsilon\delta e^2\theta^2\psi^2 - \epsilon\delta(e^2 - 4d)\theta^2\psi^2$$

est divisible par p^2. Nous avons supposé que $v_p(e) = 1$, donc $v_p(e_1) = 1$ et $v_p(e_2) = 0$. Par ailleurs, e et $\delta(e^2 - 4d)$ sont premiers entre eux. Les valuations $v_p(\delta)$ et $v_p(\mu_2)$ sont donc nulles. Par conséquent, p^2 divise ψ^4. Ce n'est pas possible : θ et ψ sont premiers entre eux. Le polynôme p ne divise donc pas θ.

Si p divise ψ : D'après la congruence 4.11, p divise ν. En fait, p^2 divise ν^2, $\delta e^2\theta^2\psi^2$, $\delta(e^2 - 4d)\theta^2\psi^2$ et $\delta e_1 e_2^2\mu_2\psi^4$. Nous en déduisons que le polynôme

$$\epsilon^2\mu\theta^4 = \epsilon\nu^2 - \epsilon\delta e^2\theta^2\psi^2 - \epsilon\delta(e^2 - 4d)\theta^2\psi^2 - \delta e_1 e_2^2\mu_2\psi^4$$

est divisible par p^2. Or $v_p(\mu) = 1$ (car μ est sans facteur carré), donc p divise θ^4. Ce n'est pas possible : θ et ψ sont premiers entre eux. Le polynôme p ne

divise donc pas ψ.

Finalement, p ne divise pas $\theta\psi$. Par ailleurs, le polynôme $-\delta d$ n'est pas un carré modulo p. Nous aboutissons ainsi à une contradiction avec la congruence 4.11 : comme p ne divise pas $\theta\psi$, la congruence 4.11 se réécrit $-\delta d \sim 1 \bmod p$. De cette contradiction, nous déduisons qu'il n'existe aucun facteur carré commun à μ et e : le polynôme μ est donc un diviseur de $\delta(e^2 - 4d)$. $\square$

Le lemme suivant est donné dans un cadre plus général que celui de la courbe elliptique précédemment étudiée.

Proposition 4.3.3 *Soit k un corps de caractéristique 0. Soit $(e_i)_{i=1}^r$ une famille d'éléments de $k[x]$. Soit P_1, $P_2 \in k[x][y]$ deux polynômes. Nous supposons que*

* *le polynôme P_2 est de degré impair en y,*
* *$\deg_y(P_1) < 2r$, et*
* *$P_2(y)\left(\left(\prod_{i=1}^r (y - e_i)\right)^2 - DP_1(y)\right)$ est sans facteur carré.*

Nous notons $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = P_2(y)\left(\left(\prod_{i=1}^r (y - e_i)\right)^2 - DP_1(y)\right).$$

Soit $p \in k[x]$ un facteur premier de D. Nous supposons que $v_p(P_2(e_i)) = 0$ pour tout $i \in \{1, \cdots, r\}$.

Soient $div(u, w)$ un diviseur semi-réduit de poids 1 et $\alpha \in k(x)$ l'unique racine de u. Nous supposons que $w(\alpha) \neq 0$. Nous notons $\beta := p^{-v_p(P_2(\alpha))} P_2(\alpha)$. Nous conservons la notation 4.1.

Il existe alors un entier $i \in \{1, \cdots, r\}$ tel que

$$\beta \sim 1 \bmod p \text{ ou } \beta \sim P_2(e_i) \bmod p.$$

Démonstration.

Soient $h(T) := \left(\prod_{i=1}^r (T - e_i)\right)^2 - DP_1(T)$ et $L := k(x)[T]/(h(T))$. Soit t la classe de T dans L. Soient u_0, $u_1 \in k[x]$ deux polynômes premiers entre eux tels que $\alpha = \frac{u_0}{u_1}$.

Par définition de la représentation de Mumford pour les éléments de $\mathrm{Jac}(\mathcal{H})$, nous avons

$$P_2(\alpha) N_{L/k(x)}(u) = w(\alpha)^2 \tag{4.12}$$

Comme $w(\alpha) \neq 0$ et $(u_1^r)^2 N_{L/k(x)}(u) = N_{L/k(x)}(u_1 y - u_0)$, nous déduisons de l'équation 4.12 que

$$P_2(\alpha) \sim N_{L/k(x)}(u_1 y - u_0).$$

Nous distinguons deux cas :

Le cas où p ne divise pas $\prod_{i=1}^{r}(u_0 - e_i u_1)$. De l'égalité

$$N_{L/k(x)}(u_1 y - u_0) = \left(\prod_{i=1}^{r}(u_0 - e_i u_1)\right)^2 - D u_1^{2r} P_1(\alpha)$$

nous déduisons la congruence

$$\left(\prod_{i=1}^{r}(u_0 - e_i u_1)\right)^2 - D u_1^{2r} P_1(\alpha) \equiv \left(\prod_{i=1}^{r}(u_0 - e_i u_1)\right)^2 \bmod p$$

(car p divise D). Or l'élément $\prod_{i=1}^{r}(u_0 - e_i u_1)$ est inversible modulo p, donc $v_p(N_{L/k(x)}(u_1 y - u_0)) = 0$ et $N_{L/k(x)}(u_1 y - u_0) \sim 1 \bmod p$. De plus $P_2(\alpha) \sim N_{L/k(x)}(u_1 y - u_0)$, donc la valuation $v_p(P_2(\alpha))$ est paire. Ainsi, puisque $v_p(\beta) = 0$ et $\beta \sim N_{L/k(x)}(u_1 y - u_0)$, nous avons $\beta \sim 1 \bmod p$.

Le cas où p divise $u_0 - e_i u_1$ pour un certain $i \in \{1, \cdots, r\}$. Les polynômes u_0 et u_1 sont premiers entre eux. Or $u_0 \equiv e_i u_1 \bmod p$, donc p ne divise pas u_1 (sinon p est aussi un diviseur de u_0).

Nous déduisons aussi de la congruence $u_0 \equiv u_1 e_i \bmod p$ que

$$\begin{aligned} u_1^{\deg(P_2)} P_2\left(\tfrac{u_0}{u_1}\right) &\equiv u_1^{\deg(P_2)} P_2\left(\tfrac{e_i u_1}{u_1}\right) \bmod p \\ &\equiv u_1^{\deg(P_2)} P_2(e_i) \bmod p. \end{aligned}$$

Finalement, puisque u_1 et $P_2(e_i)$ sont inversibles modulo p, la valuation $v_p(P_2(\alpha))$ est nulle et nous avons

$$\beta = P_2(\alpha) \sim P_2(e_i) \bmod p. \quad \square$$

Proposition 4.3.4 *Soit k un corps de caractéristique 0. Soient d, e, $\delta \in k[x]$ trois polynômes non nuls tels que $e^2 - 4d$ soit non nul.*

Soit $\mathcal{E}$ la courbe elliptique sur $k(x)$ d'équation de Weierstrass

$$\mathcal{E} : t^2 = s(s + \delta e^2)(s + \delta(e^2 - 4d)).$$

Nous conservons les notations 4.2 et 4.1.

Soit p un facteur premier de d. Nous supposons que e et δ ne sont pas divisibles par p.

Alors tout élément de l'image de $\gamma_{\mathcal{E}}$ est de la forme $[\mu]$ avec μ un diviseur sans facteur carré de $\delta e(e^2-4d)$ tel que

$$\mu \sim 1 \bmod p \text{ ou } \mu \sim -\delta \bmod p.$$

Démonstration.

Puisque les polynômes δ, d et e^2-4d étant non nuls, le polynôme $s(s+\delta e^2)(s+\delta(e^2-4d))$ (à coefficients dans $k(x)$) est sans facteur carré.

Nous posons $y := s+\delta(e^2-2d)$ et $z := t$. Ce faisant nous obtenons un isomorphisme entre $\mathcal{E}$ et la courbe elliptique $\mathcal{D}$ sur $k(x)$ d'équation affine

$$\mathcal{D} : z^2 = \left(y-\delta(e^2-2d)\right)\left(y^2-4\delta^2d^2\right).$$

Nous posons $P_1(y) := 4\delta^2 d$, $P_2(y) := y-\delta(e^2-2d)$ et $e_1(x)=0$.

Soit $(\lambda,\beta)\in\mathcal{E}(k(x))$. Nous posons $\Lambda := \lambda+\delta(e^2-2d)$. Alors (Λ,β) est un $k(x)$-point de $\mathcal{D}$.

Soit $\alpha := p^{-v_p(P_2(\Lambda))}P_2(\Lambda) = p^{-v_p(\Lambda-\delta(e^2-2d))}(\Lambda-\delta(e^2-2d))$. Le polynôme δe^2 est premier à p et $P_2(0) = -\delta(e^2-2d) \equiv -\delta e^2 \bmod p$, donc la valuation $v_p(P_2(0))$ est nulle. Nous faisons appel à la proposition 4.3.3 : nous avons $\alpha\sim 1 \bmod p$ ou $\alpha\sim -\delta(e^2-2d) \bmod p$, c'est-à-dire

$$\alpha \sim 1 \bmod p \text{ ou } \alpha \sim -\delta \bmod p.$$

Par ailleurs $P_2(\Lambda) = \Lambda-\delta(e^2-2d) = \lambda$, donc α est égal à $\alpha = p^{-v_p(\lambda)}\lambda$.

Les polynômes δ, e, d et e^2-4d sont non nuls. D'après la proposition 4.1.4, il existe $\mu\in k[x]$ sans facteur carré divisant $\delta^2e^2(e^2-4d)$ et deux polynômes $\theta\in k[x]$ et $\psi\in k[x]$ tels que

* $\mu\theta$ soit premier avec ψ, et
* $\lambda = \mu\frac{\theta^2}{\psi^2}$.

Le polynôme p est premier à δ et e et il divise d, donc p est premier à $\delta^2e^2(e^2-4d)$. Par suite, la valuation $v_p(\mu)$ est nulle, et donc

$$\alpha = p^{-v_p(\lambda)}\lambda = \mu\left(\frac{p^{-v_p(\theta)}\theta}{p^{-v_p(\psi)}\psi}\right)^2.$$

Nous en déduisons que $\mu\sim\alpha \bmod p$ (car $p^{-v_p(\theta)}\theta$ et $p^{-v_p(\psi)}\psi$ sont inversibles modulo p). Par conséquent, nous avons

$$\mu\sim 1 \bmod p \text{ ou } \mu\sim -\delta \bmod p. \qquad \square$$

Proposition 4.3.5 *Soient η, ω, $\rho\in\mathbb{R}$ des réels. Soit $k := \mathbb{Q}(\eta,\omega,\rho)$. Nous posons :*

$$b_1 = \frac{\rho^2-\eta^2}{\omega^2-\eta^2}+\frac{\eta^2-\omega^2}{4}.$$

Soient $B(x) := (x+b_1)^2 - \eta^2$ *et* $C(x) := 2(x+b_1) + \omega^2 - \eta^2 - 1$.

À tout $\zeta \in k^\times$, *nous associons la* $k(x)$*-courbe elliptique* $\widehat{\mathcal{C}}_\zeta^-$ *d'équation affine*

$$\widehat{\mathcal{C}}_\zeta^- : t^2 = s\left(s + \zeta\,(1-C)^2\right)\left(s + \zeta\left((1-C)^2 - 4\,(B-C)\right)\right).$$

Nous conservons les notations 4.2 et 4.1. Nous supposons que l'élément

$$\left(\omega^2 - \eta^2\right)^2 - 4\omega^2 = \left(\omega^2 - \eta^2 - 2\omega\right)\left(\omega^2 - \eta^2 + 2\omega\right)$$

est strictement positif.

Alors, pour tout $\zeta \in k$ *strictement positif, l'image de* $\gamma_{\widehat{\mathcal{C}}_\zeta^-,k(x)}$ *est le sous-groupe de* $k(x)^\times/k(x)^{\times 2}$ *engendré par les classes* $[-\zeta]$ *et* $\left[(1+C)^2 - 4B\right]$, *et est donc l'image des points de* 2*-torsion de* $\widehat{\mathcal{C}}_\zeta^-(k(x))$.

Démonstration.

Soit $\zeta \in k$ strictement positif. Nous appliquons les propositions 4.3.2 et 4.3.4 avec $e = 1 - C$, $d = B - C$ et $\delta = \zeta$.

Soient Λ un élément de l'image de $\gamma_{\widehat{\mathcal{C}}_\zeta^-,k(x)}$.

Les polynômes $e = 1 - C$ et $d = B - C$ étant respectivement de degrés 1 et 2, ils sont non nuls.

Puisque $\left(\omega^2 - \eta^2\right)^2 > 4\omega^2$, l'élément $\omega^2 - \eta^2$ est non nul. Ainsi, le polynôme

$$\begin{aligned} e^2 - 4d &= (1-C)^2 - 4(B-C) \\ &= (1+C)^2 - 4B \\ &= 4\left(\omega^2 - \eta^2\right)(x + b_1) + \left(\omega^2 - \eta^2\right)^2 + 4\eta^2 \\ &= 4\left(\omega^2 - \eta^2\right)x + 4\rho^2 \end{aligned}$$

est non nul. En particulier, comme $\delta = \zeta \in k^\times$ est non nul, le polynôme

$$s\left(s + \zeta\,(1-C)^2\right)\left(s + \zeta\left((1-C)^2 - 4\,(B-C)\right)\right)$$

est sans facteur carré.

Le polynôme e est de degré 1. Il est donc sans facteur carré.

Nous avons supposé $(\omega^2 - \eta^2)^2 - 4\omega^2$ strictement positif. Comme $\zeta > 0$, l'élément $-\zeta((\omega^2 - \eta^2)^2 - 4\omega^2)$ est strictement négatif. Par suite, le reste

$$\frac{-\zeta\left(\left(\omega^2 - \eta^2\right)^2 - 4\omega^2\right)}{4}$$

de la division euclidienne de $-\delta d = -\zeta(B-C) = -\zeta\left((x + b_1 - 1)^2 - \omega^2\right)$ par $e = 1 - C = -2\left(x + b_1 - 1 + \frac{\omega^2 - \eta^2}{2}\right)$ n'est pas un carré dans k (le corps

k est un sous-corps de $\mathbb{R}$). Ainsi, d'après la proposition 4.3.2, il existe un diviseur sans facteur carré μ de $\delta(e^2-4d) = \zeta\left((1+C)^2-4B\right)$ tel que $\Lambda = [\mu]$.

La classe $\gamma_{\mathcal{E}}(0,0) = \left[e^2-4d\right] = \left[(1+C)^2-4B\right]$ est un élément de l'image de $\gamma_{\widehat{\mathcal{C}}_\zeta^-}$. Quitte à ajouter cette classe à Λ, nous pouvons donc supposer, sans perte de généralité, que μ est un élément de k (le polynôme $e^2-4d = (1+C)^2-4B \in k[x]$ est de degré 1).

Le reste de la division euclidienne de $d = B-C = (x+b_1-1)^2-\omega^2$ par $e = 1-C = -2(x+b_1-1)-\left(\omega^2-\eta^2\right)$ est $\frac{\left(\omega^2-\eta^2\right)^2-4\omega^2}{4}$. Ce reste est non nul (il est même strictement positif). Par conséquent, les polynômes $d = B-C$ et $e = 1-C$ sont premiers entre eux. Ainsi, la proposition 4.3.4 s'applique et affirme que

$$\mu \sim 1 \bmod p \text{ ou } \mu \sim -\zeta \bmod p$$

pour tout facteur premier p de $d = B-C$. La constante $\mu \in k^\times$ étant égale à sa réduction modulo $B-C$, nous avons $\mu \sim 1$ ou $\mu \sim -\zeta$. $\square$

Proposition 4.3.6 *Soient η, ω, $\rho \in \mathbb{R}$ des réels. Soit $k := \mathbb{Q}(\eta,\omega,\rho)$. Nous posons :*

$$b_1 = \frac{\rho^2-\eta^2}{\omega^2-\eta^2} + \frac{\eta^2-\omega^2}{4}.$$

Soient $B(x) := (x+b_1)^2-\eta^2$ et $C(x) := 2(x+b_1)+\omega^2-\eta^2-1$. Nous supposons que les éléments $\omega^2-\eta^2$, et ρ sont non nuls.

À tout $\zeta \in k^\times$, nous associons la $k(x)$-courbe elliptique $\widehat{\mathcal{C}}_{\zeta x}^-$ d'équation affine

$$\widehat{\mathcal{C}}_{\zeta x}^- : t^2 = s\left(s+\zeta x(1-C)^2\right)\left(s+\zeta x\left((1-C)^2-4(B-C)\right)\right).$$

Nous conservons les notations 4.2 et 4.1. Nous supposons que les éléments

- $(b_1-1)^2-\omega^2$,
- $\left(\omega^2-\eta^2\right)^2-4\omega^2$
- $2(1-C(0))(1-b_1-\omega) = 2\left(2b_1-2+\omega^2-\eta^2\right)(b_1-1+\omega)$,
- $2(1-C(0))(1-b_1+\omega) = 2\left(2b_1-2+\omega^2-\eta^2\right)(b_1-1-\omega)$ *et*
- $\left((b_1-1)^2-\omega^2\right)\left(\left(\omega^2-\eta^2\right)^2-4\omega^2\right)$

ne sont pas des carrés dans k.

Alors, pour tout $\zeta \in k$ strictement positif, l'image de $\gamma_{\widehat{\mathcal{C}}_{\zeta x}^-,k(x)}$ est le sous-groupe de $k(x)^\times/k(x)^{\times 2}$ engendré par les classes $[-\zeta x]$ et $\left[(1+C)^2-4B\right]$, et est donc l'image des points de 2-torsion de $\widehat{\mathcal{C}}_{\zeta x}^-(k(x))$.

Démonstration.

Soit $\zeta \in k$ strictement positif. Nous appliquons les propositions 4.1.4, 4.3.2 et 4.3.4 avec $e = 1 - C$, $d = B - C$ et $\delta = \zeta x$.

Les polynômes $\delta = \zeta x$ et $e = 1 - C$ étant de degrés 1, ils sont non nuls. De même, le polynôme $d = B - C$ étant de degré 2, il est non nul.

L'élément $\omega^2 - \eta^2$ est non nul. Ainsi, le polynôme

$$\begin{aligned} e^2 - 4d = (1-C)^2 - 4(B-C) &= (1+C)^2 - 4B \\ &= 4\left(\omega^2 - \eta^2\right)(x + b_1) + \left(\omega^2 - \eta^2\right)^2 + 4\eta^2 \\ &= 4\left(\omega^2 - \eta^2\right)x + 4\rho^2 \end{aligned}$$

est de degré 1. Ce polynôme est donc non nul. Nous posons

* $S = 2\zeta x\left((1-C)^2 - 2(B-C)\right)$ et
* $T = \zeta^2 x^2 (1-C)^2\left((1-C)^2 - 4(B-C)\right)$.

Nous venons de montrer que le polynôme

$$\begin{aligned} T(S^2 - 4T) &= 16\delta^4 e^2 (e^2 - 4d) d^2 \\ &= 16\zeta^4 x^4 (1-C)^2\left((1-C)^2 - 4(B-C)\right)(B-C)^2 \in k[x] \end{aligned}$$

est non nul. Nous pouvons donc appliquer la proposition 4.1.4 au cas de la courbe $\widehat{\mathcal{C}^-_{\zeta x}}$.

Soit Λ un élément de l'image de $\gamma_{\widehat{\mathcal{C}^-_{\zeta x}}}$. D'après la proposition 4.1.4, il existe un diviseur sans facteur carré $\mu \in k[x]$ de

$$\begin{aligned} \delta e\left(e^2 - 4d\right) &= \zeta x(1-C)\left((1-C)^2 - 4(B-C)\right) \\ &= \zeta x(1-C)\left((1+C)^2 - 4B\right) \end{aligned}$$

tel que $\Lambda = [\mu]$.

Nous vérifions maintenant que les hypothèses des propositions 4.3.2 et 4.3.4 sont satisfaites.

Le reste de la division euclidienne de $d = B - C = (x + b_1 - 1)^2 - \omega^2$ par $e = 1 - C = -2(x + b_1 - 1) - \left(\omega^2 - \eta^2\right)$ est $\frac{\left(\omega^2-\eta^2\right)^2 - 4\omega^2}{4}$. Ce reste est non nul. Par conséquent les polynômes $B - C$ et $1 - C$ sont premiers entre eux. De même, $d(0) = B(0) - C(0) = (b_1 - 1)^2 - \omega^2$ est non nul (ce n'est pas un carré dans k) donc ζx est premier à $B - C$. Les hypothèses de la proposition 4.3.4 sont donc bien vérifiées.

Le polynôme $e = 1 - C$ est de degré 1. Il est donc non nul et sans facteur carré. Pour pouvoir appliquer la proposition 4.3.2, il est nécessaire et suffisant de montrer que $-\delta d = -\zeta x(B - C)$ n'est pas un carré modulo $e = 1 - C$.

Le reste de la division euclidienne de

$$-\delta d = -\zeta x(B-C) = -\zeta x\left((x+b_1-1)^2-\omega^2\right)$$

par $1-C=-2\left(x+b_1-1+\frac{\omega^2-\eta^2}{2}\right)$ est

$$\frac{-\zeta\left(1-C(0)\right)\left(\left(\omega^2-\eta^2\right)^2-4\omega^2\right)}{8}.$$

Ce reste est un carré dans k si et seulement si

$$-\zeta \sim 2\left(1-C(0)\right)\left(\left(\omega^2-\eta^2\right)^2-4\omega^2\right).$$

Nous devons donc distinguer deux cas suivant la valeur de ζ.

Le cas où $-2\zeta\left(1-C(0)\right)\left(\left(\omega^2-\eta^2\right)^2-4\omega^2\right)\notin k^{\times 2}$**.** Alors la proposition 4.3.2 s'applique. Nous déduisons de cette proposition que le polynôme sans facteur carré μ est un diviseur de $\delta(e^2-d)=\zeta x\left((1+C)^2-4B\right)$.

Les classes $\gamma_{\mathcal{E}}\left(-\zeta x\left(1-C\right)^2,0\right)=[-\zeta x]$ et $\gamma_{\mathcal{E}}\left(0,0\right)=\left[(1+C)^2-4B\right]$ sont des éléments de l'image de $\gamma_{\widehat{\mathcal{C}^-_{\zeta x}}}$. Quitte à ajouter l'une de ces deux classes à Λ (ou les deux), nous pouvons supposer, sans perte de généralité, que μ est un élément de k.

Le polynôme $d=B-C=(x+b_1-1)^2-\omega^2$ a deux facteurs premiers : $p_1:=x+b_1-1-\omega$ et $p_2:=x+b_1-1+\omega$. La proposition 4.3.4 affirme l'existence, pour $i\in\{1,2\}$, d'un entier $m_i\in\{0,1\}$ tel que

$$\begin{array}{l}\mu\sim(-\zeta x)^{m_1} \bmod p_1 \sim \left(-\zeta\left(1-b_1+\omega\right)\right)^{m_1} \bmod p_1\\ \mu\sim(-\zeta x)^{m_2} \bmod p_2 \sim \left(-\zeta\left(1-b_1-\omega\right)\right)^{m_2} \bmod p_2.\end{array} \tag{4.13}$$

Si $m_i=0$ **pour un certain** $i\in\{1,2\}$**.** La constante $\mu\in k$ étant égale à sa réduction modulo p_i, l'équivalence 4.13 associée à p_i signifie que $\mu\sim 1$, c'est-à-dire $\Lambda=[1]$.

Si $m_1=m_2=1$ En multipliant les deux équivalences 4.13, nous obtenons

$$\mu^2\sim(-\zeta)^2\left((1-b_1)^2-\omega^2\right).$$

Ce cas n'est pas possible car $(1-b_1)^2-\omega^2$ n'est pas un carré dans k.

Le cas où $-\zeta\sim 2\left(1-C(0)\right)\left(\left(\omega^2-\eta^2\right)^2-4\omega^2\right)$**.** Les deux classes $\gamma_{\mathcal{E}}\left(-\zeta x\left(1-C\right)^2,0\right)=[-\zeta x]$ et $\gamma_{\mathcal{E}}\left(0,0\right)=\left[(1+C)^2-4B\right]$ sont des

éléments de l'image de $\gamma_{\widehat{\mathcal{C}^-_{\zeta x}}}$. Quitte à ajouter l'une de ces deux classes à Λ (ou les deux), nous pouvons supposer sans perte de généralité que μ est un diviseur de $e = (1 - C)$.

Le polynôme $d = B - C = (x + b_1 - 1)^2 - \omega^2$ a deux facteurs premiers : $p_1 := x + b_1 - 1 - \omega$ et $p_2 := x + b_1 - 1 + \omega$.
D'après la proposition 4.3.4, il existe, pour tout $i \in \{1, 2\}$, un entier $m_i \in \{0, 1\}$ tel que

$$\begin{array}{l} \mu \sim (-\zeta x)^{m_1} \bmod p_1 \sim (-\zeta\,(1 - b_1 + \omega))^{m_1} \bmod p_1 \\ \mu \sim (-\zeta x)^{m_2} \bmod p_2 \sim (-\zeta\,(1 - b_1 - \omega))^{m_2} \bmod p_2 \end{array} \tag{4.14}$$

Nous distinguons deux sous-cas.

Si μ est une constante. Alors μ est égal à sa réduction modulo p_i. Par conséquent, les équations 4.14 signifient que
* $\mu \sim 1$ ou
* $\mu \sim -\zeta\,(1 - b_1 + \omega)$ et $\mu \sim -\zeta\,(1 - b_1 - \omega)$.
Dans le second cas, nous avons $1 \sim (1 - b_1)^2 - \omega^2$. Ce n'est pas possible. Nous avons donc $\mu \sim 1$, c'est-à-dire $\Lambda = [1]$.

S'il existe $\epsilon \in k^\times$ tel que $\mu = \epsilon(1 - C)$. Nous utilisons l'égalité $1 - C = \eta^2 - \omega^2 - 2(x + b_1 - 1)$ pour montrer les relations de congruence

$$\begin{array}{l} \mu \equiv \epsilon\left(\eta^2 - \omega^2 - 2\omega\right) \bmod p_1 \text{ et} \\ \mu \equiv \epsilon\left(\eta^2 - \omega^2 + 2\omega\right) \bmod p_2. \end{array}$$

Les équations 4.14 se reformulent alors sous la forme

$$\begin{array}{l} \epsilon\left(\eta^2 - \omega^2 - 2\omega\right) \sim (-\zeta\,(1 - b_1 + \omega))^{m_1} \text{ et} \\ \epsilon\left(\eta^2 - \omega^2 + 2\omega\right) \sim (-\zeta\,(1 - b_1 - \omega))^{m_2}. \end{array}$$

Nous en déduisons l'équivalence

$$\left(\left(\eta^2 - \omega^2\right)^2 - 4\omega^2\right) \sim (-\zeta)^{m_1 + m_2}\,(1 - b_1 + \omega)^{m_1}\,(1 - b_1 - \omega)^{m_2}.$$

Cette équivalence est en contradiction avec les hypothèses de la proposition, puisque $-\zeta \sim 2\,(1 - C(0))\left(\left((\omega^2 - \eta^2\right)^2 - 4\omega^2\right)$. Le cas où $\mu = \epsilon(1 - C)$ pour un certain $\epsilon \in k^\times$ n'est donc pas possible. □

4.4 Etude de l'image de $\Pi_{\mathcal{C}^+_\delta}$.

4.4.1 La forme générale des courbes étudiées.

Soit k un sous corps de $\mathbb{R}$. Soient D, E, $\delta \in k[x]$ trois polynômes tel que le polynôme

$$(y + \delta(1 - E))\,(y - \delta E)\,(y + \delta E)\left(y^2 - \delta^2 D\right)$$

soit sans facteur carré. Nous considérons la courbe hyperelliptique $\mathcal{H}$ d'équation affine

$$\mathcal{H} : z^2 = (y + \delta(1-E))\,(y - \delta E)\,(y + \delta E)\left(y^2 - \delta^2 D\right).$$

Notations 4.4.1.1 Nous notons
* $f_1(y) := y + \delta(1-E)$,
* $f_2(y) := y - \delta E$,
* $f_3(y) := y + \delta E$ et
* $f_4(y) := y^2 - \delta^2 D$.

Nous supposons que le polynôme $f_1 f_2 f_3 f_4$ est sans facteur carré. Nous supposons aussi que D n'est pas un carré dans $k(x)$.

Pour tout $i \in \{1,2,3,4\}$ nous posons $K_i := k(x)[y]/(f_i(y))$ et nous notons y_i la classe de y dans K_i. Soit $\pi_{\mathcal{H}} : \mathrm{Jac}(\mathcal{H})(k(x)) \longrightarrow \prod_{i=1}^{4} K_i^\times / K_i^{\times 2}$ le morphisme de Cassels-Schaefer et $\pi_{\mathcal{H},i} : \mathrm{Jac}(\mathcal{H})(k(x)) \longrightarrow K_i^\times / K_i^{\times 2}$ sa i-ème composante.

La norme $N_{K_i/k(x)}$ de l'extension $K_i/k(x)$ induit un homomorphisme $N_{K_i/k(x)} : K_i^\times / K_i^{\times 2} \longrightarrow k(x)^\times / k(x)^{\times 2}$. Nous posons $\Xi_{\mathcal{H},i} := N_{K_i/k(x)} \circ \pi_{\mathcal{H},i}$ et nous notons $\Xi_{\mathcal{H}} : \mathrm{Jac}(\mathcal{H})(k(x)) \longrightarrow \prod_{i=1}^{4} k(x)^\times / k(x)^{\times 2}$ l'homomorphisme de i-ème coordonnée $\Xi_{\mathcal{H},i}$.

Dans cette section, nous étudions l'image de $\Xi_{\mathcal{H}}$. Nous appliquons ensuite les résultats de l'étude aux cas particuliers où
* $E = \frac{1-C}{2}$,
* $D = \frac{(1+C)^2 - 4B}{4}$ et
* $\delta = \zeta$ ou $\delta = \zeta x$ pour un certain $\zeta \in k^\times$ strictement positif

Nous en déduisons en particulier des informations sur l'image des morphismes $\Pi_{\mathcal{C}_\zeta^+}$ et $\Pi_{\mathcal{C}_{\zeta x}^+}$.

Proposition 4.4.1.2 *Soit k un corps de caractéristique 0. Soient E, D, $\delta \in k[x]$ trois polynômes non nuls tels que $1-2E$, $(1-E)^2 - D$ et $E^2 - D$ soient non nuls.*

Alors le polynôme $(y + \delta(1-E))(y - \delta E)(y + \delta E)(y^2 - \delta^2 D)$ est sans facteur carré.

Démonstration.

Par hypothèse, l'élément

$$(-\delta(1-E) - \delta E)(-\delta(1-E) + \delta E)(\delta^2(1-E)^2 - \delta^2 D) = \delta^4(1-2E)((1-E)^2 - D)$$

est non nul. Par conséquent les polynômes $(y - \delta E)(y + \delta E)(y^2 - \delta^2 D)$ et $y + \delta(1-E)$ sont premiers entre eux.

De même, l'élément

$$(\delta E + \delta(1-E))(\delta E + \delta E)(\delta^2 E^2 - \delta^2 D) = 2\delta^4 E(E^2 - D)$$

est non nul, donc les polynômes $y - \delta E$ et $(y + \delta(1-E))(y + \delta E)(y^2 - \delta^2 D)$ sont premiers entre eux.

Nous avons aussi supposé que l'élément

$$(-\delta E + \delta(1-E))(-\delta E - \delta E)(\delta^2 E^2 - \delta^2 D) = -2\delta^4 E(1-2E)(E^2 - D)$$

est non nul, donc les polynômes $y - \delta E$ et $(y + \delta(1-E))(y + \delta E)(y^2 - \delta^2 D)$ sont premiers entre eux.

De ces trois relations de primalité nous déduisons aussi que les polynômes $(y + \delta(1-E))(y - \delta E)(y + \delta E)$ et $y^2 - \delta^2 D$ sont premiers entre eux.

Par ailleurs, $\delta^2 D$ est non nul, donc le polynôme $y^2 - \delta^2 D$ est sans facteur carré. Ainsi le polynôme $(y + \delta(1-E))(y - \delta E)(y + \delta E)(y^2 - \delta^2 D)$ est bien sans facteur carré. □

Proposition 4.4.1.3 *Soit k un corps de caractéristique 0. Soient E, D, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-2E$, $(1-E)^2 - D$ et $E^2 - D$ soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y + \delta(1-E))(y - \delta E)(y + \delta E)(y^2 - \delta^2 D).$$

Nous reprenons les notations 4.4.1.1. Nous supposons que $(1-E)^2 - D$ et $E^2 - D$ ne sont pas des carrés dans $k(x)$, que E et D sont de degré impairs et que δ est non nul.

Alors l'image par $\Xi_{\mathcal{H}}$ de la torsion de $Jac(\mathcal{H})(k(x))$ est l'image par $\Xi_{\mathcal{H}}$ de la 2-torsion de $Jac(\mathcal{H})(k(x))$. Elle est donc engendrée par les classes :

1. $\left([\delta], \left[2E\left(E^2 - D\right)\right], [2\delta E], \left[E^2 - D\right]\right)$,
2. $\left([1-2E], \left[-\delta\left(E^2 - D\right)\right], \left[-\delta(1-2E)\left(E^2 - D\right)\right], [1]\right)$ *et*
3. $\left(\left[(1-E)^2 - D\right], \left[E^2 - D\right], \left[E^2 - D\right], \left[(1-E)^2 - D\right]\right)$.

Démonstration.

Puisque δ, $(1-E)^2 - D$, E, $1-2E$, D et $E^2 - D$ sont non nuls, le polynôme

$$(y + \delta(1-E))(y - \delta E)(y + \delta E)(y^2 - \delta^2 D)$$

est bien sans facteur carré (voir la proposition 4.4.1.2).

Nous avons supposé que D n'est pas un carré dans $k(x)$ (il est de degré impair) et que δ est non nul. Le polynôme $(y^2 - \delta^2 D)$ est donc irréductible. Ainsi, d'après la proposition 1.4.12, la 2-torsion de $\mathrm{Jac}(\mathcal{H})(k(x))$ est engendrée par les points

1. $< y + \delta(1-E), 0 >$,

2. $< y - \delta E, 0 >$,

3. $< y + \delta E, 0 >$ et

4. $< y^2 - \delta^2 D >$.

En fait trois de ces points suffisent à engendrer la 2-torsion. Nous calculons maintenant l'image par $\Xi_{\mathcal{H}}$ de $< y + \delta(1-E), 0 >$, $< y + \delta E, 0 >$ et $< y - \delta E, 0 >$. Nous savons que

* $\Xi_{\mathcal{H},2}(< y + \delta(1-E), 0 >) = [-\delta]$,
* que $\Xi_{\mathcal{H},3}(< y + \delta(1-E), 0 >) = [\delta(2E-1)]$,
* et que $\Xi_{\mathcal{H},4}(< y + \delta(1-E), 0 >) = [\delta^2((1-E)^2 - D)]$.

Nous souhaitons calculer $\Xi_{\mathcal{H},1}(< y + \delta(1-E), 0 >)$. D'après la proposition 1.5.9, le produit des composantes de $\Xi_{\mathcal{H}}$ (qui sont toutes à valeurs dans $k(x)^{\times}/k(x)^{\times 2}$) est la classe triviale, donc l'image $\Xi_{\mathcal{H}}(< y + \delta(1-E), 0 >)$ est égale à la classe

$$\left(\left[(1-2E)((1-E)^2 - D)\right], [-\delta], [-\delta(1-2E)], \left[(1-E)^2 - D\right]\right).$$

Nous montrons de même que

$$\Xi_{\mathcal{H}}(< y - \delta E, 0 >) = \left([\delta], [2E(E^2 - D)], [2\delta E], [E^2 - D]\right) \text{ et}$$

$$\Xi_{\mathcal{H}}(< y + \delta E, 0 >) = \left([\delta(1-2E)], [-2\delta E], [-2E(1-2E)(E^2 - D)], [(E^2 - D)]\right).$$

1. Pour tout $T \in \mathrm{Jac}(\mathcal{H})(k(x))$, l'image $\Xi_{\mathcal{H}}(2T)$ est triviale. Or les images $\Xi_{\mathcal{H}}(< y + \delta(1-E), 0 >)$, $\Xi_{\mathcal{H}}(< y - \delta E, 0 >)$, et $\Xi_{\mathcal{H}}(< y + \delta E, 0 >)$ ne sont pas triviales (car $E^2 - D$ et $(1-E)^2 - D$ ne sont pas des carrés dans $k(x)$), donc les points $< y + \delta(1-E), 0 >$, $< y + \delta E, 0 >$ et $< y - \delta E, 0 >$ ne sont pas des doubles dans $\mathrm{Jac}(\mathcal{H})(k(x))$.

2. De même, le polynôme $2E$ n'est pas un carré dans $k(x)$ (il est de degré impair), donc l'image

$$\begin{array}{rcl} \Xi_{\mathcal{H},2}(< (y + \delta(1-E)), 0 > + < (y + \delta E), 0 >) & = & [-\delta][-2\delta E] \\ & = & [2E] \end{array}$$

n'est pas triviale. Par conséquent, le point $< (y + \delta(1-E))(y + \delta E), 0 >$ n'appartient pas à $2\mathrm{Jac}(\mathcal{H})(k(x))$.

3. Les polynômes E et $1-2E$ sont premiers entre eux et le polynôme E n'est pas un carré dans $k(x)$ (il est de degré impair). En utilisant la décomposition en facteurs premiers dans $k[x]$, nous en déduisons que $-2E(1-2E)$ n'est pas un carré dans $k(x)$. Par ailleurs, nous avons

$$\Xi_{\mathcal{H},3}(< y + \delta(1-E), 0 > + < y - \delta E, 0 >) = [-2E(1-2E)].$$

Ainsi, l'image de $< y+\delta(1-E), 0 > + < y-\delta E, 0 >$ par $\Xi_{\mathcal{H},3}$ n'est pas triviale et donc $< y+\delta(1-E), 0 > + < y-\delta E, 0 >$ n'appartient pas à $2\mathrm{Jac}(\mathcal{H})(k(x))$.

4. Nous savons que $\Xi_{\mathcal{H},1}(< (y+\delta E), 0 > + < (y-\delta E), 0 >) = [1-2E]$. Or $1-2E$ n'est pas un carré dans $k(x)$ (il est de degré impair), donc $< (y+\delta E), 0 > + < (y-\delta E), 0 >$ n'est pas un double dans $\mathrm{Jac}(\mathcal{H})(k(x))$.

5. Nous avons supposé que le polynôme $(1-E)^2 - D$ n'est pas un carré dans $k(x)$. L'image $\Xi_{\mathcal{H},1}(< y^2 - \delta^2 D, 0 >) = [(1-E)^2 - D]$ n'est donc pas triviale. Par suite, le point $< y^2 - \delta^2 D, 0 >$ n'appartient pas à $2\mathrm{Jac}(\mathcal{H})(k(x))$.

La 4-torsion de $\mathrm{Jac}(\mathcal{H})(k(x))$ est donc égale à sa 2-torsion. Nous en déduisons que la torsion 2-primaire $\mathrm{Jac}(\mathcal{H})(k(x))$ est égale à sa 2-torsion.

Comme l'image d'un double par $\Xi_{\mathcal{H}}$ est triviale, nous avons, pour tout entier $m \in \mathbb{N}$ impair, l'égalité $\Xi_{\mathcal{H}}(T) = \Xi_{\mathcal{H}}(mT)$. En particulier, pour tout $m \in \mathbb{N}$ impair, tout $n \in \mathbb{N}$ et tout point de $2^n m$-torsion T, l'image $\Xi_{\mathcal{H}}(T)$ est l'image du point de 2^n-torsion mT par $\Xi_{\mathcal{H}}$. Ainsi, l'image de la torsion de $\mathrm{Jac}(\mathcal{H})(k(x))$ par $\Xi_{\mathcal{H}}$ est l'image de la torsion 2-primaire, c'est-à-dire l'image de la 2-torsion. Cette image est donc engendrée par $\Xi_{\mathcal{H}}(< y+\delta(1-E), 0 >)$, $\Xi_{\mathcal{H}}(< y+\delta E, 0 >)$ et $\Xi_{\mathcal{H}}(< y-\delta E, 0 >)$, ou, de façon équivalente, par les images

* $\Xi_{\mathcal{H}}\left(< y-\delta E, 0 >\right) = \left([\delta], [2E(E^2-D)], [2\delta E], [E^2-D]\right)$,

* $\Xi_{\mathcal{H}}\left(< y+\delta E, 0 > + < y-\delta E, 0 >\right)$
  $= \left([1-2E], [-\delta(E^2-D)], [-\delta(1-2E)(E^2-D)], [1]\right)$, et

* $\Xi_{\mathcal{H}}\left(< y+\delta(1-E), 0 > + < y+\delta E, 0 > + < y-\delta E, 0 >\right)$
  $= \left([(1-E)^2-D], [E^2-D], [E^2-D], [(1-E)^2-D]\right)$ $\square$

4.4.2 Quelques applications des résultat de la section 4.1.

Proposition 4.4.2.1 *Soit k un corps de caractéristique 0. Soient E, D, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-2E$, $(1-E)^2-D$ et E^2-D soient non nuls. Nous supposons que D n'est pas un carré dans $k(x)$.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D).$$

Nous reprenons les notations 4.4.1.1. Nous supposons que

* *les polynômes $(1-E)^2-D$ et $1-2E$ sont premiers entre eux,*
* *les polynômes $(1-E)^2-D$ et E sont premiers entre eux,*

* *les polynômes* $1-2E$ *et* D *sont premiers entre eux, et*
* *les polynômes* E *et* D *sont premiers entre eux.*

Alors tout élément α *de l'image de* $\Xi_{\mathcal{H}}$ *est de la forme*

$$\alpha = ([\mu_{1,3}\mu_{1,4}], [\mu_{2,3}], [\mu_{1,3}\mu_{2,3}\mu_{3,4}], [\mu_{1,4}\mu_{3,4}]) \text{ avec}$$

* $\mu_{1,3} \in k[x]$ *un diviseur de* $\delta(1-2E)$,
* $\mu_{1,4} \in k[x]$ *un diviseur de* $\delta((1-E)^2 - D)$,
* $\mu_{2,3} \in k[x]$ *un diviseur de* $\delta E(E^2 - D)$, *et*
* $\mu_{3,4} \in k[x]$ *un diviseur de* $\delta(E^2 - D)$.

Démonstration.

Puisque δ, $(1-E)^2 - D$, E, $1-2E$, D et $E^2 - D$ sont non nuls, le polynôme

$$(y + \delta(1-E))(y - \delta E)(y + \delta E)(y^2 - \delta^2 D)$$

est bien sans facteur carré (voir la proposition 4.4.1.2).

Nous utilisons la proposition 4.1.3. Cela nous amène à considérer les polynômes

$$\Delta_{i,j} := \begin{cases} N_{K_i/k(x)}(f_j) \text{ si } j \neq i \\ N_{K_i/k(x)}(f_i') \text{ si } j = i \end{cases}$$

c'est-à-dire les polynômes suivants :

* $\Delta_{1,1} = N_{K_1/k(x)}(1) = 1$,
* $\Delta_{1,2} = -\Delta_{2,1} = N_{K_1/k(x)}(y - \delta E) = -\delta$,
* $\Delta_{1,3} = -\Delta_{3,1} = N_{K_1/k(x)}(y + \delta E) = -\delta(1-2E)$,
* $\Delta_{1,4} = \Delta_{4,1} = N_{K_1/k(x)}\left(y^2 - \delta^2 D\right) = \delta^2\left((1-E)^2 - D\right)$,
* $\Delta_{2,2} = N_{K_2/k(x)}(1) = 1$,
* $\Delta_{2,3} = -\Delta_{3,2} = N_{K_2/k(x)}(y + \delta E) = 2\delta E$,
* $\Delta_{2,4} = \Delta_{4,2} = N_{K_2/k(x)}\left(y^2 - \delta^2 D\right) = \delta^2\left(E^2 - D\right)$,
* $\Delta_{3,3} = N_{K_3/k(x)}(1) = 1$,
* $\Delta_{3,4} = \Delta_{4,3} = N_{K_3/k(x)}\left(y^2 - \delta^2 D\right) = \delta^2\left(E^2 - D\right)$, et
* $\Delta_{4,4} = N_{K_4/k(x)}(2y) = -4\delta^2 D$.

Soit α un élément de l'image de $\Xi_{\mathcal{H}}$. D'après la proposition 4.1.3, il existe une famille $(\mu_{i,j})_{\substack{1 \leq i \leq 4, \\ j \neq i}}$ d'éléments de $k[x]$ sans facteur carré telle que

* $\mu_{i,j}$ divise $\operatorname{pgcd}\left(\prod_{k=1}^{4} \Delta_{i,k}, \prod_{l=1}^{4} \Delta_{j,l}\right)$,
* $\mu_{i,j} = \mu_{j,i}$, et
* $\Xi_{\mathcal{H},i}(\alpha)$ soit la classe de $\prod_{j \neq i} \mu_{i,j}$.

1. Le polynôme $\mu_{1,3}$ divise

$$\operatorname{pgcd}\left(\delta^4(1-2E)\left((1-E)^2 - D\right), 2\delta^4 E(1-2E)\left(E^2 - D\right)\right).$$

Puisque $E^2 - D \equiv 2E - 1 \bmod \left((1-E)^2 - D\right)$ et puisque les polynômes $1-2E$ et $(1-E)^2 - D$ sont premiers entre eux, le polynôme $(1-E)^2 - D$ est premier à $E^2 - D$. Le polynôme $(1-E)^2 - D$ est aussi premier à E. Or le polynôme $\mu_{1,3}$ est sans facteur carré, donc $\mu_{1,3}$ divise $\delta(1-2E)$.

2. Le polynôme $\mu_{1,2}$ divise

$$\operatorname{pgcd}\left(\delta^4(1-2E)\left((1-E)^2 - D\right), 2\delta^4 E\left(E^2 - D\right)\right).$$

Comme $E^2 - D \equiv (1-E)^2 - D \bmod (1-2E)$, et comme $1-2E$ est premier à $(1-E)^2 - D$, les polynômes $1-2E$ et $E^2 - D$ sont premiers entre eux. Par ailleurs, $1-2E$ est premier à E, et nous avons vu que $(1-E)^2 - D$ est premier à $E\left(E^2 - D\right)$. Ainsi, le polynôme $\mu_{1,2}$ étant sans facteur carré, il divise δ.

3. Le polynôme $\mu_{1,4}$ divise

$$\operatorname{pgcd}\left(\delta^4(1-2E)\left((1-E)^2 - D\right), -4\delta^8\left((1-E)^2 - D\right)\left(E^2 - D\right)^2 D\right).$$

Nous avons vu que $1-2E$ est premier à $\left(E^2 - D\right)$. De plus, les polynômes D et $1-2E$ sont premiers entre eux. Par conséquent, le polynôme $\mu_{1,4}$ étant sans facteur carré, il divise $\delta\left((1-E)^2 - D\right)$.

4. Le polynôme $\mu_{2,3}$ divise

$$\operatorname{pgcd}\left(2\delta^4 E\left(E^2 - D\right), 2\delta^4 E(1-2E)\left(E^2 - D\right)\right)$$

et est sans facteur carré. Le polynôme $\mu_{2,3}$ divise donc $\delta E\left(E^2 - D\right)$.

5. Le polynôme $\mu_{2,4}$ divise

$$\operatorname{pgcd}\left(2\delta^4 E\left(E^2 - D\right), -4\delta^8\left((1-E)^2 - D\right)\left(E^2 - D\right)^2 D\right).$$

Les polynômes E et $\left((1-E)^2 - D\right)D$ sont premiers entre eux. Ainsi, le polynôme $\mu_{2,4}$ étant sans facteur carré, il divise $\delta\left(E^2 - D\right)$.

6. Le polynôme $\mu_{3,4}$ divise

$$\operatorname{pgcd}\left(2\delta^4 E(1-2E)\left(E^2 - D\right), -4\delta^8\left((1-E)^2 - D\right)\left(E^2 - D\right)^2 D\right).$$

Par hypothèse, les polynômes $E(1-2E)$ et $\left((1-E)^2 - D\right)D$ sont premiers entre eux. Comme le polynôme $\mu_{3,4}$ est sans facteur carré, $\mu_{3,4}$ divise $\delta\left(E^2 - D\right)$.

Nous souhaitons maintenant montrer qu'il est possible de choisir les $\mu_{i,j}$ tels que $\mu_{1,2} = \mu_{2,4} = 1$. Pour cela, nous remplaçons $\mu_{i,j}$ par la partie sans facteur carré de $\widetilde{\mu}_{i,j}$ avec

* $\widetilde{\mu}_{1,2} = 1$, $\widetilde{\mu}_{1,3} = \mu_{1,3}\mu_{1,2}$, $\widetilde{\mu}_{1,4} = \mu_{1,4}$,
* $\widetilde{\mu}_{2,3} = \mu_{2,3}\mu_{1,2}\mu_{2,4}$, $\widetilde{\mu}_{2,4} = 1$ et $\widetilde{\mu}_{3,4} = \mu_{3,4}\mu_{2,4}$.

Avec ces notations, nous avons bien

* $\widetilde{\mu}_{1,3}\widetilde{\mu}_{1,4} = \mu_{1,3}\mu_{1,2}\mu_{1,4}$,
* $\widetilde{\mu}_{2,3} = \mu_{2,3}\mu_{1,2}\mu_{2,4}$,
* $\begin{aligned}\widetilde{\mu}_{1,3}\widetilde{\mu}_{2,3}\widetilde{\mu}_{3,4} &= (\mu_{1,3}\mu_{1,2})(\mu_{2,3}\mu_{1,2}\mu_{2,4})(\mu_{3,4}\mu_{2,4}) \\ &= (\mu_{1,2}\mu_{2,4})^2(\mu_{1,3}\mu_{2,3}\mu_{3,4}),\text{ et}\end{aligned}$
* $\widetilde{\mu}_{1,4}\widetilde{\mu}_{3,4} = \widetilde{\mu}_{1,4}\mu_{3,4}\mu_{2,4}$

c'est-à-dire

$$\Xi_{\mathcal{H}}(\alpha) = ([\widetilde{\mu}_{1,3}\widetilde{\mu}_{1,4}], [\widetilde{\mu}_{2,3}], [\widetilde{\mu}_{1,3}\widetilde{\mu}_{2,3}\widetilde{\mu}_{3,4}], [\widetilde{\mu}_{1,4}\widetilde{\mu}_{3,4}]).$$

Nous remarquons aussi que

* $\widetilde{\mu}_{1,3} \in k[x]$ est un diviseur de $\delta(1-2E)$, (car $\mu_{1,2}$ est un diviseur de δ et $\mu_{1,3}$ est un diviseur de $\delta(1-2E)$),
* $\widetilde{\mu}_{1,4} \in k[x]$ est un diviseur de $\delta((1-E)^2 - D)$,
* $\widetilde{\mu}_{2,3} \in k[x]$ un diviseur de $\delta E(E^2-D)$, (car $\mu_{1,2}$ est un diviseur de δ, $\mu_{2,3}$ est un diviseur de $\delta E(E^2-D)$ et $\mu_{2,4}$ est un diviseur de $\delta\left(E^2-D\right)$), et
* $\widetilde{\mu}_{3,4} \in k[x]$ un diviseur de $\delta(E^2-D)$ (car $\mu_{2,4}$ est un diviseur de $\delta\left(E^2-D\right)$ et $\mu_{3,4} \in k[x]$ est un diviseur de $\delta(E^2-D)$). □

Proposition 4.4.2.2 *Soit k un corps de caractéristique 0. Soient E, D, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-2E$, $(1-E)^2-D$ et E^2-D soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y+\delta(1-E))(y-\delta E)(y+\delta E)\left(y^2-\delta^2 D\right).$$

Nous reprenons les notations 4.4.1.1 et 4.1. Nous supposons que

* *les hypothèses de la proposition 4.4.2.1 sont vérifiées,*
* *D est de degré impair.*

Soit λ le coefficient dominant de D.

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\epsilon_1\alpha_1], [\epsilon_2\alpha_2], [\epsilon_3\alpha_3], [\epsilon_4\alpha_4])$$

avec α_1, α_2, α_3, $\alpha_4 \in k[x]$ quatre polynômes unitaires et ϵ_1, ϵ_2, ϵ_3, $\epsilon_4 \in k^\times$ tels que

* *$\epsilon_4 \sim 1$ si α_4 est de degré pair ;*
* *$\epsilon_4 \sim -\lambda$ si α_4 est de degré impair.*

Démonstration.

Puisque δ, $(1-E)^2-D$, E, $1-2E$, D et E^2-D sont non nuls, le polynôme

$$(y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D)$$

est bien sans facteur carré (voir la proposition 4.4.1.2).

Soit $\mathrm{div}(u,v) \in \mathrm{Div}^0(k(\mathcal{H}))$ un diviseur semi-réduit avec $u(y)$ premier à $f_4(y) = y^2 - \delta^2 D$. Nous notons $\mathrm{Cl}(\mathrm{div}(u,v))$ la classe d'équivalence linéaire de $\mathrm{div}(u,v)$. Nous avons alors $\Xi_{\mathcal{H},4}(\mathrm{Cl}(\mathrm{div}(u,v))) = \left[N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right)\right]$. Il existe un polynôme unitaire $\alpha_4 \in k[x]$ et $\epsilon_4 \in k^\times$ tels que

$$N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right) = \epsilon_4\alpha_4.$$

Nous appliquons la proposition 4.1.6 en prenant pour $\mathcal{P}$ la place à l'infini de $k(x)$ et à $A := \delta^2 D$: comme $A \sim D$, et comme D est de degré impair et de coefficient dominant λ, nous avons

* $\epsilon_4 \sim 1$ si α_4 est de degré pair ;
* $\epsilon_4 \sim -\lambda$ si α_4 est de degré impair. $\square$

Proposition 4.4.2.3 *Soit k un corps de caractéristique 0. Soient E, D, $\delta \in k[x]$ trois polynômes non nuls tels que les éléments $1-2E$, $(1-E)^2 - D$ et $E^2 - D$ soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y + \delta(1-E))\,(y - \delta E)\,(y + \delta E)\left(y^2 - \delta^2 D\right).$$

Nous reprenons les notations 4.4.1.1 et 4.1. Nous supposons que les hypothèses de la proposition 4.4.2.1 sont vérifiées.
Soit p un facteur premier de D. Nous supposons que

* *la valuation $v_p(D)$ est impaire, et*
* *$v_p(\delta) = v_p(E) = v_p(1-E) = 0$.*

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\alpha_1], [\alpha_2], [\alpha_3], [\alpha_4])$$

avec α_1, α_2, α_3, $\alpha_4 \in k[x]$ quatre polynômes tels que

$$v_p(\alpha_4) = 0 \text{ et } \alpha_4 \sim 1 \bmod p.$$

Démonstration.

Puisque δ, $(1-E)^2 - D$, E, $1-2E$, D et $E^2 - D$ sont non nuls, le polynôme

$$(y + \delta(1-E))(y - \delta E)(y + \delta E)(y^2 - \delta^2 D)$$

est bien sans facteur carré (voir la proposition 4.4.1.2).

Soit $\mathrm{div}(u,v) \in \mathrm{Div}^0(k(\mathcal{H}))$ un diviseur semi-réduit avec u premier à $f_4(y) := y^2 - \delta^2 D$. Nous notons $\mathrm{Cl}(\mathrm{div}(u,v))$ la classe d'équivalence linéaire de $\mathrm{div}(u,v)$. Nous avons alors $\Xi_{\mathcal{H},4}(\mathrm{Cl}(\mathrm{div}(u,v))) = \left[N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right)\right]$. Nous posons

$$\alpha_4 := p^{-v_p(N_{K_4/k(x)}((-1)^{\deg(u)}u))} N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right).$$

D'après la proposition 4.4.2.1, la classe $\left[N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right)\right]$ est la classe d'un diviseur sans facteur carré μ de $\delta\left((1-E)^2-D\right)\left(E^2-D\right)$. Nous avons supposé que $v_p(\delta)=v_p(E)=v_p(1-E)=0$. Ainsi, la valuation $v_p(\mu)$ est paire. Or $N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right)$ est le produit de μ par un élément de $k(x)^{\times 2}$, donc la valuation $v_p\left(N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right)\right)$ est paire. Nous en déduisons que $N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right)\sim\alpha_4$, c'est-à-dire que

$$[\alpha_4]=\left[N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right)\right]=\Xi_{\mathcal{H},4}(\mathrm{Cl}(\mathrm{div}(u,v))).$$

Nous appliquons la proposition 4.1.6 en prenant pour $\mathcal{P}$ la place associée à p et à $A:=\delta^2D$: comme la valuation $v_p(\delta^2D)$ est impaire, et comme la valuation $v_p(\alpha_4)$ est nulle, nous avons $\alpha_4\sim 1 \bmod p$. □

4.4.3 Deux propositions techniques.

Lemme 4.4.3.1 *Soit k un corps de caractéristique 0. Soient E, D, $\delta\in k[x]$ trois polynômes non nuls tels que les polynômes $1-2E$, $(1-E)^2-D$ et E^2-D soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H}: z^2=(y+\delta(1-E))\,(y-\delta E)\,(y+\delta E)\left(y^2-\delta^2D\right).$$

Nous reprenons les notations 4.4.1.1. Soit $\alpha\in Jac(\mathcal{H})(k(x))$ un $k(x)$-point de $Jac(\mathcal{H})$. Soit $p\in k[x]$ un facteur premier de E. Nous supposons que

- $v_p(E)\equiv 1 \bmod 2$,
- $v_p(\delta)\equiv 0 \bmod 2$, *et*
- $v_p(E^2-D)\equiv 0 \bmod 2$.

Il existe alors un point de 2-torsion $T\in Jac(\mathcal{H})(k(x))_{tors}$ et un élément $<u,v>$ de $Jac(\mathcal{H})(k(x))$ tels que

1. $\alpha=T+<u,v>$,
2. *u est de degré au plus 2,*
3. *u est premier à $(y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2D)$, et*
4. *(a)* $v_p(u(\delta E))\equiv 0 \bmod 2$, *ou*
   (b) $\deg(u)\leq 1$ *et* $v_p(u(\delta E))\equiv 1 \bmod 2$.

Démonstration.

Puisque δ, $(1-E)^2-D$, E, $1-2E$, D et E^2-D sont non nuls, le polynôme

$$(y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2D)$$

est bien sans facteur carré (voir la proposition 4.4.1.2).

Soit $\mathrm{div}(u_\alpha, v_\alpha)$ un diviseur semi-réduit de classe d'équivalence linéaire égale à α tel que u_α soit premier à $(y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D)$. Le quadruplet

$$\Xi_{\mathcal{H}}(< y-\delta E, 0 >) = \left([\delta], [2E(E^2-D)], [2\delta E], [E^2-D]\right)$$

est un élément de l'image de la 2-torsion de $\mathrm{Jac}(\mathcal{H})(k(x))$ par $\Xi_{\mathcal{H}}$. Or $v_p(E) \equiv 1 \bmod 2$ et $v_p(\delta) \equiv v_p(E^2-D) \bmod 2 \equiv 0 \bmod 2$, donc il existe un point de 2-torsion $T \in \mathrm{Jac}(\mathcal{H})(k(x))_{tors}$ et une famille $(\alpha_i)_{i=1}^4$ d'éléments non nuls de $k[x]$ tels que

* $\Xi_{\mathcal{H}}(T) = ([\alpha_1], [\alpha_2], [\alpha_3], [\alpha_4])$, et
* $v_p(\alpha_2) \equiv v_p(u_\alpha(\delta E)) \bmod 2$

(en fait nous choisissons $T =< y-\delta E, 0 >$ si la valuation $v_p(u_\alpha(\delta E))$ est impaire, et nous prenons $T = 0$ si la valuation $v_p(u_\alpha(\delta E))$ est paire).

Soit $(\widetilde{u}, \widetilde{v})$ la représentation de Mumford de $\alpha + T$. Le point $\alpha + T =< \widetilde{u}, \widetilde{v} >$ satisfait aux conditions 1, 2 et 4 (a) du lemme. Malheureusement, le polynôme $\widetilde{u}$ n'est pas toujours premier à

$$(y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D)$$

et la condition 3 du lemme n'est donc pas toujours satisfaite. Nous décidons donc de noter

* $u_f := \mathrm{pgcd}\left(\widetilde{u}, (y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D)\right)$,
* u l'unique polynôme unitaire défini par $\widetilde{u} = u_f u$ et
* v le reste de la division euclidienne de $\widetilde{v}$ par u.

Le point $T+ < u_f, 0 >$ est un point de 2-torsion. Le point $< u, v >= \alpha + T- < u_f, 0 >$ satisfait donc aux conditions 1, 2 et 3 du lemme.

Lorsque $\deg(u_f) = 0$**.** Le point $< u, v >=< \widetilde{u}, \widetilde{v} >= \alpha + T$ satisfait à la condition 4 (a) du lemme. Il vérifie donc les conditions 1, 2, 3 et 4 (a).

Lorsque $\deg(u_f) = 1$**.** Nous avons deux sous cas.

Lorsque $v_p(u(\delta E)) \equiv 0 \bmod 2$**.** Alors $< u, v >= \alpha + T+ < u_f, 0 >$ satisfait aux conditions 1, 2, 3 et 4 (a) du lemme.

Lorsque $v_p(u(\delta E)) \equiv 1 \bmod 2$**.** Alors $< u, v >= \alpha + T+ < u_f, 0 >$ satisfait aux conditions 1, 2, 3 et 4 (b) du lemme.

Lorsque $\deg(u_f) = 2$**.** Le point $< \widetilde{u}, \widetilde{v} >$ est un point de 2-torsion. Le point $< u, v >=< 1, 0 >= 0$ satisfait aux conditions 1, 2, 3 et 4 (a) du lemme. □

Proposition 4.4.3.2 *Soit k un corps de caractéristique 0. Soient E, D, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-2E$, $(1-E)^2-D$ et E^2-D soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D).$$

Nous reprenons les notations 4.4.1.1. Nous supposons que les hypothèses de la proposition 4.4.2.1 sont vérifiées.

Soit p un facteur premier de E. Nous supposons que

$$v_p(E) = 1 \text{ et } v_p(\delta) = v_p(D) = v_p((1-E)^2 - D) = 0.$$

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\alpha_1], [\alpha_2], [\alpha_3], [\alpha_4])$$

avec α_1, α_2, α_3, $\alpha_4 \in k[x]$ quatre polynômes tels que

1. *$\alpha_2\alpha_3 \sim 1 \bmod p$ si $v_p(\alpha_2) \equiv 0 \bmod 2$, et*
2. *$\alpha_2\alpha_3 \sim -\delta D \bmod p$ si $v_p(\alpha_2) \equiv 1 \bmod 2$.*

Démonstration.

L'idée de cette démonstration est d'utiliser l'égalité

$$u(-\delta E) = u(\delta E) - 2\delta E u_1 \tag{4.15}$$

1. Une simplification du problème.

Puisque δ, $(1-E)^2 - D$, E, $1-2E$, D et $E^2 - D$ sont non nuls, le polynôme

$$(y + \delta(1-E))(y - \delta E)(y + \delta E)(y^2 - \delta^2 D)$$

est bien sans facteur carré (voir la proposition 4.4.1.2).

Nous notons $\mathcal{S}$ l'ensemble des $\alpha = ([\alpha_1], [\alpha_2], [\alpha_3], [\alpha_4]) \in \left(k(x)^\times / k(x)^{\times 2}\right)^4$ avec α_1, α_2, α_3, $\alpha_4 \in k[x]$ quatre polynômes tels que

* $\alpha_2\alpha_3 \sim 1 \bmod p$ si $v_p(\alpha_2) \equiv 0 \bmod 2$, et
* $\alpha_2\alpha_3 \sim -\delta D \bmod p$ si $v_p(\alpha_2) \equiv 1 \bmod 2$.

Soit β un $k(x)$-point de $\mathrm{Jac}(\mathcal{H})$. Nous souhaitons montrer que $\Xi_{\mathcal{H}}(\beta) \in \mathcal{S}$.

D'après le lemme 4.4.3.1, il existe un point de 2-torsion $T \in \mathrm{Jac}(\mathcal{H})(k(x))_{tors}$ et un élément $< \widetilde{u}, \widetilde{v} >$ de $\mathrm{Jac}(\mathcal{H})(k(x))$ tels que

1. $\beta = T + < \widetilde{u}, \widetilde{v} >$,
2. $\widetilde{u}$ est de degré au plus 2,
3. $\widetilde{u}$ est premier à $(y + \delta(1-E))(y - \delta E)(y + \delta E)(y^2 - \delta^2 D)$, et
4. (a) $v_p(\widetilde{u}(\delta E)) \equiv 0 \bmod 2$, ou
   (b) $\deg(\widetilde{u}) \leq 1$ et $v_p(\widetilde{u}(\delta E)) \equiv 1 \bmod 2$.

Puisque $\Xi_{\mathcal{H}}$ est un homomorphisme et puisque les images des points de 2-torsion de $\mathrm{Jac}(\mathcal{H})(k(x))$ par $\Xi_{\mathcal{H}}$ appartiennent à $\mathcal{S}$, l'image $\Xi_{\mathcal{H}}(\beta)$ appartient à $\mathcal{S}$ si et seulement si $\Xi_{\mathcal{H}}(\beta + T)$ appartient à $\mathcal{S}$.

2. Nous nous ramenons à un problème dans $k[x]$.

Il existe quatre polynômes u_0, u_1, u_2, $\lambda \in k[x]$ premiers dans leur ensemble tels que

$$\widetilde{u}(y) = \frac{u_2}{\lambda}y^2 + \frac{u_1}{\lambda}y + \frac{u_0}{\lambda}.$$

Puisque $\widetilde{u}$ est unitaire, λ est le coefficient dominant du polynôme $u(y) := u_2y^2 + u_1y + u_0$. Ainsi λ est égal à u_2, u_1 ou u_0. Par conséquent, les polynômes u_2, u_1 et u_0 sont premiers entre eux dans leur ensemble.

Nous montrons que la valuation $v_p(\lambda)$ est paire. Pour cela, nous supposons que la valuation $v_p(\lambda)$ est impaire. Le polynôme $\lambda \in k[x]$ est le coefficient dominant de $u(y)$. Nous avons donc deux possibilités

* le polynôme $u(y)$ est de degré au plus 1 et alors u_2 est nul, ou
* le polynôme $u(y)$ est de degré 2 et alors $u_2 = \lambda$.

Dans les deux cas, p divise le polynôme $u_2 \in k[x]$.

D'après la proposition 4.4.2.1, nous avons $[\widetilde{u}\,(\delta\,(E-1))] = [\mu_{1,3}\mu_{1,4}]$ avec

* $\mu_{1,3}$ un diviseur sans facteur carré de $\delta(1-2E)$, et
* $\mu_{1,4}$ un diviseur sans facteur carré de $\delta\left((1-E)^2 - D\right)$.

Les polynômes E et $1-2E$ sont premiers entre eux. Nous avons conservé les hypothèses de la proposition 4.4.2.1. En particulier, les polynômes E et $(E-1)^2 - D$ sont premiers entre eux. Ainsi, puisque p divise E et $v_p(\delta) = 0$, les polynômes $\mu_{1,3}$ et $\mu_{3,4}$ sont premiers à p. Or $[\widetilde{u}\,(\delta\,(E-1))] = [\mu_{1,3}\mu_{1,4}]$, donc la valuation $v_p(\widetilde{u}(\delta(E-1)))$ est paire. Par suite, la valuation

$$v_p(u(\delta(E-1))) = v_p(\widetilde{u}(\delta(E-1))) + v_p(\lambda)$$

est impaire. De plus, $u(\delta(E-1))$ est un élément de $k[x]$, donc le polynôme p divise $u(\delta(E-1))$. Ainsi, le polynôme p divisant E et u_2, nous avons

$$\begin{aligned} u(\delta(E-1)) &= u_2\delta^2(E-1)^2 + u_1\delta(E-1) + u_0 \\ &\equiv -\delta u_1 + u_0 \bmod p. \end{aligned}$$

Nous en déduisons la congruence $u_0 \equiv \delta u_1 \bmod p$. Or u_2, u_1 et u_0 sont premiers entre eux dans leur ensemble et p divise u_2, donc p ne divise pas u_1. En particulier, p divisant λ, le polynôme λ n'est ni u_1 ni u_0 et est donc u_2. Le polynôme u_2 est alors de valuation impaire en p et est donc non nul : le polynôme $\widetilde{u}(y)$ est de degré 2.

Puisque le polynôme $\widetilde{u}(y)$ est de degré 2, la condition 4.(a) de la définition du polynôme $\widetilde{u}$ impose à la valuation $v_p(\widetilde{u}(\delta E))$ d'être paire. Par suite, la valuation

$$v_p(u(\delta E)) = v_p(\widetilde{u}(\delta E)) + v_p(\lambda)$$

est impaire.

Par ailleurs, comme δ est premier à p et

$$\begin{aligned} u(\delta E) &= u_2\delta^2E^2 + u_1\delta E + u_0 \\ &\equiv u_0 \bmod p \\ &\equiv \delta u_1 \bmod p, \end{aligned}$$

la valuation $v_p(u(\delta E))$ est nulle. De cette contradiction, nous déduisons que la valuation $v_p(\lambda)$ est paire.

3. Nous montrons la proposition.

Nous venons de montrer que les valuations $v_p(u(\delta E))$ et $v_p(\widetilde{u}(\delta E))$ ont même parité. Nous montrons la proposition en différenciant trois cas suivant la valuation $v_p(u(\delta E))$.

Le cas où u est de degré au plus 2 premier à $f_{\mathcal{H}}$, et $v_p(\widetilde{u}(\delta E))$ est paire. Alors la valuation $v_p(u(\delta E))$ est paire.

Lorsque $v_p(u(\delta E)) = 0$. Le polynôme p divise E. Ainsi, de l'équation 4.15 nous déduisons la congruence

$$u(\delta E) \equiv u(-\delta E) \bmod p.$$

Or $u(\delta E)$ est inversible modulo p, donc

$$u(\delta E)u(-\delta E) \sim 1 \bmod p.$$

Pour conclure, il suffit de remarquer que

$$\begin{aligned} \Xi_{\mathcal{H},2}(\beta+T)\Xi_{\mathcal{H},3}(\beta+T) &= \left[(-1)^{\deg(\widetilde{u})}\widetilde{u}(\delta E)(-1)^{\deg(\widetilde{u})}\widetilde{u}(-\delta E)\right] \\ &= \left[\lambda^{-2}u(\delta E)u(-\delta E)\right] \\ &= \left[u(\delta E)u(-\delta E)\right]. \end{aligned}$$

Lorsque $v_p(u(\delta E)) \geq 1$. La valuation $v_p(u(\delta E))$ est paire. Elle est donc supérieure ou égale à 2. Nous faisons appel à la proposition 4.4.2.1 : nous avons

$$\Xi_{\mathcal{H}}(\beta) = ([\mu_{1,3}\mu_{1,4}], [\mu_{2,3}], [\mu_{1,3}\mu_{2,3}\mu_{3,4}], [\mu_{1,4}\mu_{3,4}]) \text{ avec}$$

* $\mu_{1,3} \in k[x]$ un diviseur de $\delta(1-2E)$,
* $\mu_{1,4} \in k[x]$ un diviseur de $\delta((1-E)^2 - D)$,
* $\mu_{2,3} \in k[x]$ un diviseur de $\delta E(E^2 - D)$, et
* $\mu_{3,4} \in k[x]$ un diviseur de $\delta(E^2 - D)$.

Nous avons conservé les hypothèses de la proposition 4.4.2.1. En particulier, les polynômes

* E et $(1-E)^2 - D$ sont premiers entre eux, et
* E et $E^2 - D$ sont premiers entre eux (car E et D sont premiers entre eux).

Nous avons aussi supposé que E et δ sont premiers entre eux. Enfin, les polynômes E et $1-2E$ sont premiers entre eux. Par suite les valuations $v_p(\mu_{1,3})$, $v_p(\mu_{1,4})$ et $v_p(\mu_{3,4})$ sont nulles. Ainsi, comme $[u(\delta E)] = [\mu_{2,3}]$ et $[u(-\delta E)] = [\mu_{1,3}\mu_{2,3}\mu_{3,4}]$, nous avons

$$v_p(u(-\delta E)) \equiv v_p(u(\delta E)) \bmod 2 \equiv 0 \bmod 2.$$

Or l'élément $u(-\delta E) = u(\delta E) - 2\delta E u_1$ est divisible par p (car p divise E), donc la valuation $v_p(u(-\delta E))$ est supérieure ou égale à 2. Par conséquent, p^2 divise

$$2\delta E u_1 = u(\delta E) - u(-\delta E).$$

En particulier, p divise u_1 (car $v_p(\delta E) = 1$). Finalement p est un facteur commun à u_1 et $u_0 = u(\delta E) - \delta E u_1 - \delta^2 E^2 u_2$, donc

* les polynômes u_2 et p sont premiers entre eux (car u_0, u_1 et u_2 sont premiers entre eux),
* $(-1)^{\deg(u)}\lambda u(\delta(E-1)) \equiv \delta^2(E-1)^2 u_2^2 \bmod p$ (car $\lambda = u_2$),
* $$\begin{aligned} N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right) &= \left(u_0 + \delta^2 D u_2\right)^2 - \delta^2 D u_1^2 \\ &\equiv \delta^4 D^2 u_2^2 \bmod p. \end{aligned}$$

Pour conclure nous utilisons la proposition 1.5.9 : l'image

$$\Xi_{\mathcal{H},2}(\beta+T)\Xi_{\mathcal{H},3}(\beta+T) = \Xi_{\mathcal{H},1}(\beta+T)\Xi_{\mathcal{H},4}(\beta+T)$$

est égale à la classe

$$\left[(-1)^{\deg(u)}\lambda u(\delta(E-1))N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right)\right] = [1].$$

Le cas où u est de degré 1 premier à $f_{\mathcal{H}}$, et $v_p(u(\delta E))$ est impaire.
Alors p divise $u(\delta E)$ et donc $u_0 = u(\delta E) - u_1\delta E$. Nous en déduisons deux congruences :

$$\begin{aligned} &N_{K_4/k(x)}((-1)^{\deg(u)}u) = u_0^2 - \delta^2 D u_1^2 \equiv -\delta^2 D u_1^2 \bmod p \text{ et} \\ &u(\delta(E-1)) = \delta(E-1)u_1 + u_0 \equiv -\delta u_1 \bmod p. \end{aligned}$$

Le polynôme $\widetilde{u}$ est unitaire de degré 1, donc $\lambda = u_1$. Nous avons donc $-\lambda u(\delta(E-1)) \equiv \delta u_1^2 \bmod p$. Les polynômes u_0 et u_1 étant premiers entre eux, u_1 n'est pas divisible par p. De plus $v_p(\delta) = v_p(D) = 0$, et nous pouvons donc écrire :

$$\begin{aligned} &N_{K_4/k(x)}((-1)^{\deg(u)}u) \sim -D \bmod p \text{ et} \\ &(-1)^{\deg(u)}\lambda u(\delta(E-1)) \bmod p \sim \delta \bmod p. \end{aligned}$$

Pour conclure nous utilisons la proposition 1.5.9 : l'image

$$\Xi_{\mathcal{H},2}(\beta+T)\Xi_{\mathcal{H},3}(\beta+T) = \Xi_{\mathcal{H},1}(\beta+T)\Xi_{\mathcal{H},4}(\beta+T)$$

est égale à la classe

$$\left[(-1)^{\deg(u)}\lambda u(\delta(E-1))N_{K_4/k(x)}\left((-1)^{\deg(u)}u\right)\right] = [-\delta D]. \quad \square$$

Lemme 4.4.3.3 *Soit k un corps de caractéristique 0. Soient E, D, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-2E$, $(1-E)^2-D$ et E^2-D soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y+\delta(1-E))\,(y-\delta E)\,(y+\delta E)\left(y^2-\delta^2 D\right).$$

Nous reprenons les notations 4.4.1.1. Soit $\alpha \in Jac(\mathcal{H})(k(x))$ un $k(x)$-point de $Jac(\mathcal{H})$.
Soit $p \in k[x]$ un facteur premier de E^2-D. Nous supposons que

* $v_p(E^2-D) \equiv 1 \bmod 2$,
* $v_p(E) \equiv 0 \bmod 2$,
* $v_p(2E-1) \equiv 0 \bmod 2$, *et*
* $v_p(\delta) \equiv 0 \bmod 2$.

Il existe alors un point de torsion $T \in Jac(\mathcal{H})(k(x))_{tors}$ et un élément $< u, v >$ de $Jac(\mathcal{H})(k(x))$ tels que

1. $\alpha = T + < u, v >$,
2. *u est de degré au plus* 2,
3. *u est premier à $(y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D)$, et*
4. *(a)* $v_p(u(-\delta E)) \equiv v_p(u(\delta E)) \equiv 0 \bmod 2$, *ou*
   (b) $\deg(u) \leq 1$ *et* $v_p(u(\delta E)u(-\delta E)) \equiv 1 \bmod 2$.

Démonstration.

Puisque les polynômes δ, $(1-E)^2-D$, E, $1-2E$, D et E^2-D sont non nuls, le polynôme

$$(y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D)$$

est bien sans facteur carré (voir la proposition 4.4.1.2).

Soient $(\lambda_i)_{i=1}^4$ une famille d'éléments non nuls de $k[x]$ tels que

$$\Xi_{\mathcal{H}}(\alpha) = ([\lambda_1], [\lambda_2], [\lambda_3], [\lambda_4]).$$

Les quadruplets

$$\Xi_{\mathcal{H}}\left(< y-\delta E, 0 >\right) = \left([\delta], \left[2E\left(E^2-D\right)\right], [2\delta E], \left[E^2-D\right]\right) \text{ et}$$

$$\Xi_{\mathcal{H}}\left(< y^2-\delta^2 D, 0 >\right)$$
$$= \left(\left[(1-E)^2-D\right], \left[E^2-D\right], \left[E^2-D\right], \left[(1-E)^2-D\right]\right)$$

sont des éléments de l'image de la 2-torsion de $\mathrm{Jac}(\mathcal{H})(k(x))$ par $\Xi_{\mathcal{H}}$. Or $v_p(E^2-D) \equiv 1 \bmod 2$ et $v_p(\delta) \equiv v_p(E) \bmod 2 \equiv 0 \bmod 2$, donc il existe un point de 2-torsion $T \in \mathrm{Jac}(\mathcal{H})(k(x))_{tors}$ et une famille $(\alpha_i)_{i=1}^4$ d'éléments non nuls de $k[x]$ tels que

* $\Xi_{\mathcal{H}}(T) = ([\alpha_1], [\alpha_2], [\alpha_3], [\alpha_4])$,
* $v_p(\alpha_3) \equiv v_p(\lambda_3) \bmod 2$, et
* $v_p(\alpha_2) \equiv v_p(\lambda_2) \bmod 2$.

Soit $(\widetilde{u}, \widetilde{v})$ la représentation de Mumford de $\alpha + T$. Le point $\alpha + T =< \widetilde{u}, \widetilde{v} >$ satisfait aux conditions 1, 2, et 4 (a) du lemme. Malheureusement, le polynôme $\widetilde{u}$ n'est pas toujours premier à

$$(y + \delta(1 - E))(y - \delta E)(y + \delta E)(y^2 - \delta^2 D)$$

et la condition 3 du lemme n'est donc pas toujours satisfaite. Nous décidons donc de noter

* $u_f := \text{pgcd}\left(\widetilde{u}, (y + \delta\,(1 - E))\,(y - \delta E)\,(y + \delta E)\left(y^2 - \delta^2 D\right)\right)$,
* u l'unique polynôme unitaire défini par $\widetilde{u} = u_f u$ et
* v le reste de la division euclidienne de $\widetilde{v}$ par u.

Pour conclure nous utilisons les trois affirmations suivantes :

* $\alpha = (T + < u_f, 0 >) + < u, v >$,
* $T + < u_f, 0 >$ est un point de 2-torsion, et
* u est premier au polynôme $(y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D)$.

Soit $(\beta_i)_{i=1}^4$ une famille d'éléments non nuls sans facteur carré de $k[x]$ telle que $\Xi_{\mathcal{H}}(< u_f, 0 >) = ([\beta_1], [\beta_2], [\beta_3], [\beta_4])$.

Lorsque $\deg(u_f) = 0$**.** Le point $< u, v >=< \widetilde{u}, \widetilde{v} >= \alpha + T$ satisfait aux conditions 1, 2, 3 et 4 (a) du lemme.

Lorsque $\deg(u_f) = 1$**.** Alors le polynôme $u(y) \in k(x)[y]$ est de degré 1. Nous distinguons trois sous-cas.

Lorsque $u_f = y + \delta E$**.** Nous avons

$$\begin{aligned}\Xi_{\mathcal{H},2}(< u_f, 0 >) &= [-2\delta E] \text{ et}\\ \Xi_{\mathcal{H},3}(< u_f, 0 >) &= \left[-2E(1 - 2E)\left(E^2 - D\right)\right].\end{aligned}$$

Par conséquent la valuation $v_p(\beta_2)$ est paire et la valuation $v_p(\beta_3)$ est impaire. Or

$$\begin{aligned}([u\,(\delta E)]\,, [u\,(-\delta E)]) &= (\Xi_{\mathcal{H},2}\,(< u, v >)\,, \Xi_{\mathcal{H},3}\,(< u, v >))\\ &= ([\lambda_2\alpha_2\beta_2]\,, [\lambda_3\alpha_3\beta_3])\,,\end{aligned}$$

et $v_p(\lambda_2\alpha_2) \equiv v_p(\lambda_3\alpha_3) \bmod 2 \equiv 0 \bmod 2$, donc la valuation $v_p(u(\delta E))$ est paire et la valuation $v_p(u(-\delta E))$ est impaire.

Ainsi, le point $< u, v >$ satisfait aux conditions 1, 2, 3 et 4 (b).

Lorsque $u_f = y - \delta E$**.** Nous avons

$$\begin{aligned}\Xi_{\mathcal{H},2}(< u_f, 0 >) &= \left[2E\left(E^2 - D\right)\right] \text{ et}\\ \Xi_{\mathcal{H},3}(< u_f, 0 >) &= [2\delta E].\end{aligned}$$

Par conséquent la valuation $v_p(\beta_2)$ est impaire et la valuation $v_p(\beta_3)$ est paire. Or

$$\begin{aligned}([u(\delta E)],[u(-\delta E)]) &= (\Xi_{\mathcal{H},2}(<u,v>),\Xi_{\mathcal{H},3}(<u,v>)) \\ &= ([\lambda_2\alpha_2\beta_2],[\lambda_3\alpha_3\beta_3]),\end{aligned}$$

et $v_p(\lambda_2\alpha_2) \equiv v_p(\lambda_3\alpha_3) \bmod 2 \equiv 0 \bmod 2$, donc la valuation $v_p(u(\delta E))$ est impaire et la valuation $v_p(u(-\delta E))$ est paire.

Ainsi, le point $< u, v >$ satisfait aux conditions 1, 2, 3 et 4 (b).

Lorsque u_f ne s'annule pas en δE et en $-\delta E$. Le polynôme $u(y)$ est de degré 1. Il est donc égal à $y + \delta(1-E)$. En particulier β_2 est un élément de la classe $[-\delta]$ et β_3 appartient à la classe $[-\delta(1-2E)]$. Nous déduisons que les valuations $v_p(\beta_2)$ et $v_p(\beta_3)$ sont paires. Or

$$[u(\delta E)] = \Xi_{\mathcal{H},2}(<u,v>) = [\lambda_2\alpha_2\beta_2],$$

$$[u(-\delta E)] = \Xi_{\mathcal{H},3}(<u,v>) = [\lambda_3\alpha_3\beta_3],$$

et $v_p(\lambda_2\alpha_2) \equiv v_p(\lambda_3\alpha_3) \bmod 2 \equiv 0 \bmod 2$, donc les valuations $v_p(u(\delta E))$ et $v_p(u(-\delta E))$ sont paires.

Ainsi, le point $< u, v >$ satisfait aux conditions 1, 2, 3 et 4 (a).

Lorsque $\deg(u_f) = 2$**.** Le point $< \widetilde{u}, \widetilde{v} >$ est de torsion. Le point $< u, v >=< 1, 0 >= 0$ satisfait donc aux conditions 1, 2, 3 et 4 (a). □

Proposition 4.4.3.4 *Soit k un corps de caractéristique 0. Soient E, D, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-2E$, $(1-E)^2-D$ et E^2-D soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D).$$

Nous reprenons les notations 4.4.1.1. Nous supposons que les hypothèses de la proposition 4.4.2.1 sont vérifiées.

Soit p un facteur premier de E^2-D. Nous supposons $v_p\left(E^2-D\right) = 1$ et $v_p(\delta) = v_p(E) = v_p(1-2E) = 0$.

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\alpha_1],[\alpha_2],[\alpha_3],[\alpha_4])$$

avec α_1, α_2, α_3, $\alpha_4 \in k[x]$ quatre polynômes sans facteur carré tels que

1. *$\alpha_1 \sim 1 \bmod p$ ou $\alpha_1 \sim 1-2E \bmod p$ si $v_p(\alpha_2\alpha_3) \equiv 0 \bmod 2$;*
2. *$\alpha_1 \sim \delta \bmod p$ ou $\alpha_1 \sim \delta(1-2E) \bmod p$ si $v_p(\alpha_2\alpha_3) \equiv 1 \bmod 2$.*

Démonstration.

1. Une simplification du problème.

Puisque δ, $(1-E)^2-D$, E, $1-2E$, D et E^2-D sont non nuls, le polynôme

$$(y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D)$$

est bien sans facteur carré (voir la proposition 4.4.1.2).

Nous notons $\mathcal{S}$ l'ensemble des $\alpha=([\alpha_1],[\alpha_2],[\alpha_3],[\alpha_4])\in\left(k(x)^\times/k(x)^{\times 2}\right)^4$ avec α_1, α_2, α_3, $\alpha_4\in k[x]$ quatre polynômes sans facteur carré tels que

1. $\alpha_1\sim 1 \bmod p$ ou $\alpha_1\sim 1-2E \bmod p$ si $v_p(\alpha_2\alpha_3)\equiv 0 \bmod 2$;
2. $\alpha_1\sim \delta \bmod p$ ou $\alpha_1\sim \delta(1-2E) \bmod p$ si $v_p(\alpha_2\alpha_3)\equiv 1 \bmod 2$.

Soit β un $k(x)$-point de $\mathrm{Jac}(\mathcal{H})$. Nous souhaitons montrer que $\Xi_{\mathcal{H}}(\beta)\in\mathcal{S}$.

D'après le lemme 4.4.3.3, il existe un point de 2-torsion $T\in\mathrm{Jac}(\mathcal{H})(k(x))_{tors}$ et un élément $<\widetilde{u},\widetilde{v}>$ de $\mathrm{Jac}(\mathcal{H})(k(x))$ tels que

1. $\beta=T+<\widetilde{u},\widetilde{v}>$,
2. $\widetilde{u}$ est de degré au plus 2,
3. $\widetilde{u}$ est premier à $(y+\delta(1-E))(y-\delta E)(y+\delta E)(y^2-\delta^2 D)$, et
4. (a) $v_p(\widetilde{u}(-\delta E))\equiv v_p(\widetilde{u}(\delta E)) \bmod 2\equiv 0 \bmod 2$, ou
   (b) $\deg(\widetilde{u})\leq 1$ et $v_p(\widetilde{u}(\delta E)\widetilde{u}(-\delta E))\equiv 1 \bmod 2$.

Puisque $\Xi_{\mathcal{H}}$ est un homomorphisme et puisque les images des points de 2-torsion de $\mathrm{Jac}(\mathcal{H})(k(x))$ par $\Xi_{\mathcal{H}}$ sont dans $\mathcal{S}$, l'image $\Xi_{\mathcal{H}}(\beta)$ appartient à $\mathcal{S}$ si et seulement si $\Xi_{\mathcal{H}}(\beta-T)$ appartient à $\mathcal{S}$.

2. Nous nous ramenons à un problème dans $k[x]$.

Il existe quatre polynômes u_0, u_1, u_2 et λ premiers dans leur ensemble tels que

$$\widetilde{u}(y)=\frac{u_2}{\lambda}y^2+\frac{u_1}{\lambda}y+\frac{u_0}{\lambda}.$$

Puisque $\widetilde{u}$ est unitaire, λ est le coefficient dominant du polynôme $u(y):=u_2y^2+u_1y+u_0$. Ainsi λ est égal à u_2, u_1 ou u_0. Par conséquent, les polynômes u_2, u_1 et u_0 sont premiers entre eux dans leur ensemble.

Nous montrons que la valuation $v_p(\lambda)$ est paire. Pour cela, nous supposons que la valuation $v_p(\lambda)$ est impaire. Le polynôme $\lambda\in k[x]$ est le coefficient dominant de $u(y)\in k[x][y]$. Nous avons donc deux possibilités

* le polynôme $u(y)$ est de degré au plus 1 et alors u_2 est nul, ou
* le polynôme $u(y)$ est de degré 2 et alors $u_2=\lambda$.

Dans les deux cas, p divise le polynôme $u_2\in k[x]$.

D'après la proposition 4.4.2.1, nous avons $[\widetilde{u}(\delta(E-1))]=[\mu_{1,3}\mu_{1,4}]$ avec

* $\mu_{1,3}$ un diviseur sans facteur carré de $\delta(1-2E)$, et

* $\mu_{1,4}$ un diviseur sans facteur carré de $\delta\left((1-E)^2-D\right)$.

Nous avons conservé les hypothèses de la proposition 4.4.2.1. En particulier, les polynômes $1-2E$ et E^2-D sont premiers entre eux.

De plus, nous avons $(1-E)^2-D \equiv 1-2E \bmod \left(E^2-D\right)$, donc les polynômes $(1-E)^2-D$ et E^2-D sont premiers entre eux.

Ainsi, puisque p divise E^2-D et $v_p(\delta)=0$, les polynômes $\mu_{1,3}$ et $\mu_{3,4}$ sont premiers à p. Or $[\widetilde{u}(\delta(E-1))] = [\mu_{1,3}\mu_{1,4}]$, donc la valuation $v_p(\widetilde{u}(\delta(E-1)))$ est paire. Par suite, la valuation

$$v_p(u(\delta(E-1))) = v_p(\widetilde{u}(\delta(E-1))) + v_p(\lambda)$$

est impaire. De plus $u(\delta(E-1))$ est un élément de $k[x]$. Le polynôme p divise donc $u(\delta(E-1))$.

Par ailleurs, le polynôme p divisant u_2, nous avons

$$\begin{aligned} u(\delta(E-1)) &= u_2\delta^2(E-1)^2 + u_1\delta(E-1) + u_0 \\ &\equiv \delta(E-1)u_1 + u_0 \bmod p. \end{aligned}$$

Or le polynôme p divise $u(\delta(E-1))$, donc

$$u_0 \equiv -\delta(E-1)u_1 \bmod p.$$

De cette congruence, nous déduisons que le polynôme p ne divise donc pas u_1, car :

* p divise u_2, et

* les polynômes $u_2 \in k[x]$, $u_1 \in k[x]$ et $u_0 \in k[x]$ sont premiers entre eux dans leur ensemble.

En particulier, p divisant λ, le polynôme λ n'est ni u_1 ni u_0 et est donc u_2. Le polynôme u_2 est alors de valuation impaire en p et est donc non nul : le polynôme $\widetilde{u}(y)$ est de degré 2.

Puisque le polynôme $\widetilde{u}(y)$ est de degré 2, la condition 4.(a) de la définition du polynôme $\widetilde{u}$ impose à la valuation $v_p(\widetilde{u}(\delta E))$ d'être paire. Ainsi, la valuation

$$v_p(u(\delta E)) = v_p(\widetilde{u}(\delta E)) + v_p(\lambda)$$

doit être impaire.

Par ailleurs, comme p est premier à δ et u_1, et

$$\begin{aligned} u(\delta E) &= u_2\delta^2E^2 + u_1\delta E + u_0 \\ &\equiv \delta E u_1 - \delta(E-1)u_1 \bmod p \\ &\equiv \delta u_1 \bmod p, \end{aligned}$$

la valuation $v_p(u(\delta E))$ est nulle. De cette contradiction, nous déduisons que la valuation $v_p(\lambda)$ est paire.

3. Nous montrons la proposition.

Nous considérons le polynôme $\Psi_u(T) \in k(x)[T]$ défini par

$$\begin{aligned}\Psi_u(T) &:= \mathrm{res}_y\left((-1)^{\deg(u)}u(y), y^2 - T\right)\\ &= (u_0 + Tu_2)^2 - Tu_1^2.\end{aligned}$$

Cette définition est motivée par les deux égalités

$$\Psi_u(\delta^2 D) = N_{K_4/k(x)}\left((-1)^{\deg(u)}\, u\right) = \lambda^2 N_{K_4/k(x)}\left((-1)^{\deg(\widetilde{u})}\,\widetilde{u}\right) \text{ et}$$

$$\begin{aligned}\Psi_u(\delta^2 E^2) &= (-1)^{\deg(u)}u(\delta E).(-1)^{\deg(u)}u(-\delta E).\\ &= \left((-1)^{\deg(u)}\,\lambda\widetilde{u}\,(\delta E)\right).\left((-1)^{\deg(u)}\,\widetilde{u}\,(-\delta E)\right)\end{aligned}$$

En effet, de ces égalités nous déduisons respectivement

$$\Xi_{\mathcal{H},4}\left(<\widetilde{u},\widetilde{v}>\right) = \left[\Psi_u\left(\delta^2 D\right)\right] \text{ et}$$

$$\Xi_{\mathcal{H},2}\left(<\widetilde{u},\widetilde{v}>\right).\Xi_{\mathcal{H},3}(<\widetilde{u},\widetilde{v}>) = \left[\Psi_u\left(\delta^2 E^2\right)\right].$$

Ainsi, d'après la proposition 1.5.9, l'image $\Xi_{\mathcal{H},1}\left(<\widetilde{u},\widetilde{v}>\right)$ est égale à la classe $\left[\Psi_u(\delta^2 E^2)\Psi_u(\delta^2 D)\right]$.

En appliquant la formule de Taylor au polynôme $\Psi_u(T)$ en δ^2E^2, puis en l'évaluant en $\delta^2 D$, nous montrons

$$\Psi_u\left(\delta^2 D\right) - \Psi_u\left(\delta^2 E^2\right) = \Psi_u^{'}\left(\delta^2 E^2\right)\delta^2\left(D - E^2\right) + u_2^2\delta^4\left(D - E^2\right)^2 \quad (4.16)$$

avec $\Psi_u^{'}\left(\delta^2 E^2\right) = 2u_2\left(u_0 + \delta^2 E^2 u_2\right) - u_1^2$ l'évaluation en δ^2E^2 de la dérivée (au sens usuel) $\Psi_u^{'}(T)$ du polynôme $\Psi_u(T)$. L'équation 4.16 est l'argument essentiel de la démonstration de la proposition 4.4.3.4.

Nous avons montré que la valuation $v_p(\lambda)$ est paire. Par suite,

* les valuations $v_p(u(\delta E))$ et $v_p(\widetilde{u}(\delta E))$ ont même parité ;
* les valuations $v_p(u(-\delta E))$ et $v_p(\widetilde{u}(-\delta E))$ ont même parité.

Nous montrons la proposition en différenciant plusieurs cas suivant les valuations $v_p(u(\delta E))$ et $v_p(u(-\delta E))$.

Lorsque $\widetilde{u}$ est de degré au plus 2 premier à $f_{\mathcal{H}}$ tel que les valuations $v_p(\widetilde{u}(-\delta E))$ et $v_p(\widetilde{u}(\delta E))$ soient paires.

Alors les valuations $v_p(u(\delta E))$ et $v_p(u(-\delta E))$ sont paires.

Lorsque $v_p\left(u\left(\delta E\right)\right) = v_p\left(u\left(-\delta E\right)\right) = 0$.

Alors la valuation en p de $\Psi_u\left(\delta^2 E^2\right) = u\left(\delta E\right)u\left(-\delta E\right)$ est nulle. Puisque $p|(D - E^2)$, l'équation 4.16 induit la congruence

$$\Psi_u(\delta^2 D) \equiv \Psi_u(\delta^2 E^2) \bmod p.$$

Or $\Psi_u\left(\delta^2E^2\right)$ est inversible modulo p, donc $\Psi_u\left(\delta^2D\right)$ est aussi inversible modulo p et $\Psi_u(\delta^2D)\Psi_u(\delta^2E^2) \sim 1 \bmod p$. Pour conclure il suffit de remarquer que $\Xi_{\mathcal{H},1}(< u, v >) = \left[\Psi_u(\delta^2E^2)\Psi_u(\delta^2D)\right]$.

Lorsque $v_p\left(u\left(\delta E\right)u\left(-\delta E\right)\right) \geq 1$**.**

Alors la valuation en p de $\Psi_u\left(\delta^2E^2\right) = u\left(\delta E\right)u\left(-\delta E\right)$ est strictement positive.

Puisque $p|(D - E^2)$, l'équation 4.16 induit la congruence

$$\Psi_u(\delta^2D) \equiv \Psi_u(\delta^2E^2) \bmod p.$$

En particulier, p divise $\Psi_u(\delta^2D)$.

Nous avons supposé que les valuations $v_p(\delta)$ et $v_p(1-2E)$ sont nulles. Comme $(1-E)^2 - D \equiv 1 - 2E \bmod (E^2 - D)$ et comme p divise $E^2 - D$, la valuation $v_p((1-E)^2 - D)$ est nulle. D'après la proposition 4.4.2.1, il existe donc un polynôme $\alpha_1 \in k[x]$ premier à p tel que

$$\Xi_{\mathcal{H},1}\left(< \widetilde{u}, \widetilde{v} >\right) = \left[\alpha_1\right].$$

De plus, d'après la proposition 1.5.9, nous avons $\alpha_1 \sim \Psi_u\left(\delta^2E^2\right)\Psi_u\left(\delta^2D\right)$, car

$$\Xi_{\mathcal{H},4}\left(< \widetilde{u}, \widetilde{v} >\right) = \left[\Psi_u\left(\delta^2D\right)\right] \text{ et}$$

$$\Xi_{\mathcal{H},2}\left(< \widetilde{u}, \widetilde{v} >\right).\Xi_{\mathcal{H},3}(< \widetilde{u}, \widetilde{v} >) = \left[\Psi_u\left(\delta^2E^2\right)\right].$$

La valuation $v_p(\alpha_1)$ étant nulle, les valuations $v_p\left(\Psi_u\left(\delta^2E^2\right)\right)$ et $v_p\left(\Psi_u\left(\delta^2D\right)\right)$ ont même parité.

Or la valuation en p de $\Psi_u\left(\delta^2E^2\right) = u\left(\delta E\right)u\left(-\delta E\right)$ est paire, donc $v_p\left(\Psi_u\left(\delta^2D\right)\right)$ est paire.

Finalement, les valuations $v_p\left(\Psi_u\left(\delta^2E^2\right)\right)$ et $v_p\left(\Psi_u\left(\delta^2D\right)\right)$ sont supérieures ou égales à 2. D'après l'équation 4.16, ce n'est possible que dans le cas où p divise $\Psi_u^{'}\left(\delta^2E^2\right)$, c'est-à-dire quand

$$2u_2\left(u_0 + \delta^2E^2u_2\right) - u_1^2 = \Psi_u^{'}\left(\delta^2E^2\right) \equiv 0 \bmod p. \tag{4.17}$$

Comme $\Psi_u\left(\delta^2E^2\right) = u(\delta E)u(-\delta E)$, nous sommes amenés à distinguer trois cas.

Lorsque p **divise** $u(\delta E)$ **mais pas** $u(-\delta E)$**.**

Puisque $u(\delta E) \equiv 0 \bmod p$, nous avons

$$u_0 \equiv -\delta^2E^2u_2 - \delta Eu_1 \bmod p. \tag{4.18}$$

En reportant dans la congruence 4.17 nous obtenons :

$$(-2\delta E u_2 - u_1)\, u_1 \equiv 0 \bmod p. \tag{4.19}$$

Or $2\delta E u_1 = u(\delta E) - u(-\delta E)$ et p divise $u(\delta E)$ mais pas $u(-\delta E)$, donc p ne divise pas u_1. Par suite la congruence 4.19 signifie que

$$u_1 \equiv -2\delta E u_2 \bmod p.$$

En particulier, p ne divise pas u_2.
En reportant dans la congruence 4.18, nous montrons

$$u_0 \equiv \delta^2 E^2 u_2 \bmod p.$$

En remplaçant u_0 et u_1 par leur valeurs en fonction de u_2, nous obtenons alors

$$\begin{array}{rcl} \lambda u(\delta(E-1)) & = & u_2\left(u_2\delta^2(1-E)^2 - u_1\delta(1-E) + u_0\right) \\ & \equiv & u_2^2\delta^2\left((1-E)^2 + 2(1-E)E + E^2\right) \bmod p \\ & \equiv & u_2^2\delta^2 \bmod p. \end{array}$$

Ainsi, comme u_2 et δ sont premiers à p, nous avons

$$\lambda u(\delta(E-1)) \sim 1 \bmod p,$$

ce qui permet de conclure puisque

$$\Xi_{\mathcal{H},1}(<\widetilde{u},\widetilde{v}>) = \left[(-1)^{\deg(\widetilde{u})}\,\widetilde{u}\,(\delta\,(E-1))\right] = \left[\lambda u\,(\delta\,(E-1))\right].$$

Lorsque p divise $u(-\delta E)$ mais pas $u(\delta E)$.
Puisque $u(\delta E) \equiv 0 \bmod p$, nous avons

$$u_0 \equiv -\delta^2 E^2 u_2 + \delta E u_1 \bmod p. \tag{4.20}$$

En reportant dans la congruence 4.17 nous obtenons :

$$(2\delta E u_2 - u_1)\, u_1 \equiv 0 \bmod p. \tag{4.21}$$

Or $2\delta E u_1 = u(\delta E) - u(-\delta E)$ et p divise $u(-\delta E)$ mais pas $u(\delta E)$, donc p ne divise pas u_1. Par suite l'équation 4.21 signifie que

$$u_1 \equiv 2\delta E u_2 \bmod p.$$

En particulier, p ne divise pas u_2.
En reportant dans la congruence 4.20, nous montrons

$$u_0 \equiv \delta^2 E^2 u_2 \bmod p.$$

En remplaçant u_0 et u_1 par leur valeurs en fonction de u_2, nous obtenons alors

$$\begin{aligned}\lambda u(\delta(E-1)) &= u_2\left(u_2\delta^2(1-E)^2 - u_1\delta(1-E) + u_0\right)\\ &\equiv u_2^2\delta^2\left((1-E)^2 - 2(1-E)E + E^2\right) \bmod p\\ &\equiv u_2^2\delta^2(1-2E)^2 \bmod p.\end{aligned}$$

Ainsi, comme u_2, $1-2E$ et δ sont premiers à p, nous avons

$$\lambda u(\delta(E-1)) \sim 1 \bmod p,$$

ce qui permet de conclure puisque

$$\Xi_{\mathcal{H},1}(< u, v >) = \left[(-1)^{\deg(\widetilde{u})}\widetilde{u}\left(\delta\left(E-1\right)\right)\right] = \left[\lambda u\left(\delta\left(E-1\right)\right)\right].$$

Lorsque p divise $u(\delta E)$ et $u(-\delta E)$.

Alors p divise

$$\begin{aligned}&2\delta E u_1 = u(\delta E) - u(-\delta E) \text{ et}\\ &2(\delta^2E^2u_2 + u_0) = u(\delta E) + u(-\delta E)\end{aligned}$$

et est premier à δE, donc

$$u_1 \equiv 0 \bmod p \text{ et } u_0 \equiv -\delta^2E^2u_2 \bmod p.$$

Or u_0, u_1 et u_2 sont premiers entre eux dans leur ensemble, donc p ne divise pas u_2.

Nous avons aussi

$$\begin{aligned}u(\delta(E-1)) &= u_2\delta^2(E-1)^2 + u_1\delta(E-1) + u_0\\ &\equiv u_2\delta^2\left((E-1)^2 - E^2\right) \bmod p\\ &\equiv u_2\delta^2(1-2E) \bmod p.\end{aligned}$$

Ainsi, comme u_2, δ et $(1-2E)$ sont premiers à p, nous avons

$$\lambda u(\delta(E-1)) \sim u_2^2\delta^2(1-2E) \bmod p \sim 1-2E \bmod p.$$

Pour conclure il suffit de remarquer

$$\Xi_{\mathcal{H}}(< \widetilde{u}, \widetilde{v} >) = \left[(-1)^{\deg(\widetilde{u})}\,\widetilde{u}(\delta(E-1))\right] = \left[\lambda u(\delta(E-1))\right].$$

Lorsque $\widetilde{u}$ est de degré au plus 1 premier à $f_{\mathcal{H}}$ tel que la valuation $v_p(\widetilde{u}(\delta E)\widetilde{u}(-\delta E))$ soit impaire.

Alors la valuation $v_p(u(\delta E)u(-\delta E))$ est impaire. Nous distinguons deux sous cas suivant la parité de la valuation $v_p(u(-\delta E))$.

Lorsque la valuation $v_p(u(\delta E))$ est paire et la valuation

$v_p(u(-\delta E))$ **impaire.**

Nous avons alors

$$u_0 - \delta E u_1 = u(-\delta E) \equiv 0 \bmod p. \tag{4.22}$$

Or u_0 et u_1 sont premiers entre eux, donc p ne divise pas u_1.

En utilisant la congruence 4.22 nous montrons aussi

$$\begin{aligned} -\lambda u\left(-\delta(1-E)\right) &= -u_1\left(-u_1\delta(1-E)+u_0\right) \\ &\equiv u_1^2\delta(1-2E) \bmod p. \end{aligned}$$

Nous en déduisons la relation

$$-\lambda u\left(-\delta(1-E)\right) \sim \delta(1-2E) \bmod p$$

(puisque u_1, δ et $1-2E$ sont inversibles modulo p). Pour conclure, il suffit de remarquer

$$\begin{aligned} \Xi_{\mathcal{H},1}(< u, v >) &= \left[(-1)^{\deg(u)}\lambda u(-\delta(1-E))\right] \\ &= \left[-\lambda u(-\delta(1-E))\right]. \end{aligned}$$

Lorsque la valuation $v_p(u(\delta E))$ est impaire et la valuation $v_p(u(-\delta E))$ paire.

Nous avons alors

$$u_0 + \delta E u_1 = u(\delta E) \equiv 0 \bmod p. \tag{4.23}$$

Or u_0 et u_1 sont premiers entre eux, donc p ne divise pas u_1. En utilisant la congruence 4.23, nous montrons aussi

$$\begin{aligned} -\lambda u\left(-\delta(1-E)\right) &= -u_1\left(-u_1\delta(1-E)+u_0\right) \\ &\equiv u_1^2\delta \bmod p. \end{aligned}$$

Nous en déduisons la relation

$$-\lambda u\left(-\delta(1-E)\right) \sim \delta \bmod p$$

(puisque u_1 et δ sont inversibles modulo p). Pour conclure, il suffit de remarquer

$$\begin{aligned} \Xi_{\mathcal{H},1}(< u, v >) &= \left[(-1)^{\deg(u)}\lambda u(-\delta(1-E))\right] \\ &= \left[-\lambda u(-\delta(1-E))\right]. \quad \square \end{aligned}$$

4.4.4 Application aux courbes $\mathcal{C}_\delta^+$.

Proposition 4.4.4.1 *Soient η, ω, $\rho \in \mathbb{R}$ des réels. Soit $k := \mathbb{Q}(\eta, \omega, \rho)$. Nous posons :*

$$b_1 = \frac{\rho^2 - \eta^2}{\omega^2 - \eta^2} + \frac{\eta^2 - \omega^2}{4}.$$

Soient $B(x) := (x + b_1)^2 - \eta^2$ et $C(x) := 2(x + b_1) + \omega^2 - \eta^2 - 1$. Nous supposons que les éléments

* $\left(\omega^2 - \eta^2 - 1\right)^2 - 4\eta^2$,
* $\left(\omega^2 - \eta^2 - 2\right)^2 - 4\eta^2$ *et*
* $\left(\omega^2 - \eta^2\right)^2 - 2\left(\omega^2 + \eta^2\right)$

sont non nuls.

À tout $\delta \in k(x)^\times$ nous associons la $k(x)$-courbe hyperelliptique $\mathcal{C}_\delta^+$ d'équation affine

$$\mathcal{C}_\delta^+ : z^2 = \left(y + \tfrac{\delta(1+C(x))}{2}\right)\left(y - \tfrac{\delta(1-C(x))}{2}\right)\left(y + \tfrac{\delta(1-C(x))}{2}\right)\left(y^2 - \tfrac{\delta^2((1+C(x))^2 - 4B(x))}{4}\right).$$

Nous supposons de plus $|\omega| > 1 + |\eta|$ et qu'aucun des éléments

* $\left((\omega - 1)^2 - \eta^2\right)^{n_1}\left((\omega + 1)^2 - \eta^2\right)^{n_2}$ *avec* $(n_1, n_2) \in \{(0,1), (1,0), (1,1)\}$
* $2\left(\omega^2 - \eta^2\right)\left(\omega^2 - \eta^2 - 2\omega\right)\left((\omega + 1)^2 - \eta^2\right)^n$ *(pour $n \in \{0, 1\}$) et*
* $2\left(\omega^2 - \eta^2\right)\left(\omega^2 - \eta^2 + 2\omega\right)\left((\omega - 1)^2 - \eta^2\right)^n$ *(pour $n \in \{0, 1\}$)*

n'est un carré dans k.

Alors, pour tout $\zeta \in k$ strictement positif, l'image de $\Pi_{\mathcal{C}_\zeta^+}$ est engendrée par l'image des points de torsion 2-primaire de $Jac(\mathcal{C}_\zeta^+)(k(x))$.

Démonstration.

Nous allons utiliser lors de cette démonstration les propositions 4.4.2.1, 4.4.2.2, 4.4.3.2 et 4.4.3.4 en posant $E(x) := \frac{1-C(x)}{2}$ et $D = \frac{(1+C(x))^2 - 4B(x)}{4}$. Avec ces notations, nous avons :

* $1 - E = \frac{1+C}{2}$,
* $1 - 2E = C$,
* $E^2 - D = B - C$ et
* $(1 - E)^2 - D = B$.

Nous commençons par montrer quatre relations de primalité relative.

a. Le reste de la division euclidienne de

$$(1 - E)^2 - D = B = (x + b_1)^2 - \eta^2$$

par $1 - 2E = C = 2(x + b_1) + \omega^2 - \eta^2 - 1$ est égal à

$$\frac{(\omega^2 - \eta^2 - 1)^2 - 4\eta^2}{4} = \frac{(\omega^2 - \eta^2 - 1 - 2\eta)(\omega^2 - \eta^2 - 1 + 2\eta)}{4}.$$

Ce reste est non nul par hypothèse, donc les polynômes $1-2E=C$ et $(1-E)^2-D=B$ sont premiers entre eux.

b. De même le reste

$$\frac{\left(\omega^2-\eta^2-2\right)^2-4\eta^2}{4}=\frac{(\omega^2-\eta^2-2-2\eta)(\omega^2-\eta^2-2+2\eta)}{4}$$

de la division euclidienne de $(1-E)^2-D=B=(x+b_1)^2-\eta^2$ par $E=\frac{1-C}{2}=-x-b_1+1-\frac{\omega^2-\eta^2}{2}$ est non nul, donc les polynômes $(1-E)^2-D=B$ et $E=\frac{1-C}{2}$ sont premiers entre eux.

c. Le reste de la division euclidienne de

$$4D=(1+C)^2-4B=4(\omega^2-\eta^2)(x+b_1)+(\omega^2-\eta^2)^2+4\eta^2$$

par $1-2E=C=2(x+b_1)+\omega^2-\eta^2-1$ est égal à

$$-2(\omega^2-\eta^2)(\omega^2-\eta^2-1)+(\omega^2-\eta^2)^2+4\eta^2=-(\omega^2-\eta^2)^2+2\omega^2+2\eta^2.$$

Ce reste étant non nul, les polynômes D et $1-2E$ sont premiers entre eux.

d. Les éléments $2(\omega^2-\eta^2)(\omega^2-\eta^2-2\omega)$ et $2(\omega^2-\eta^2)(\omega^2-\eta^2+2\omega)$ n'étant pas des carrés dans k, les deux éléments $\omega^2-\eta^2-2\omega$ et $\omega^2-\eta^2+2\omega$ sont non nuls. Par suite, le reste

$$-2(\omega^2-\eta^2)(\omega^2-\eta^2-2)+(\omega^2-\eta^2)^2+4\eta^2=4\omega^2-(\omega^2-\eta^2)^2$$

de la division euclidienne de

$$\begin{aligned}4D &= (1+C)^2-4B\\ &= 4\left(\omega^2-\eta^2\right)(x+b_1)+\left(\omega^2-\eta^2\right)^2+4\eta^2\end{aligned}$$

par $E=\frac{1-C}{2}=-x-b_1+1-\frac{\omega^2-\eta^2}{2}$ est non nul. Les les polynômes D et E sont donc premiers entre eux.

Par ailleurs $\omega^2>\eta^2$ (car $|\omega|>1+|\eta|$), donc le polynôme

$$\begin{aligned}4D &= (1+C)^2-4B\\ &= 4\left(\omega^2-\eta^2\right)(x+b_1)+\left(\omega^2-\eta^2\right)^2+4\eta^2\end{aligned}$$

est de degré 1. Par conséquent, le polynôme D n'est pas un carré dans $k(x)$. Les hypothèses de la proposition 4.4.2.1 sont donc vérifiées.

En particulier, les polynômes $(1-E)^2-D$, E, $1-2E$, D et E^2-D sont non nuls. Or $\delta=\zeta\in k^\times$ est non nul, donc le polynôme

$$\left(y+\tfrac{\delta(1+C(x))}{2}\right)\left(y-\tfrac{\delta(1-C(x))}{2}\right)\left(y+\tfrac{\delta(1-C(x))}{2}\right)\left(y^2-\tfrac{\delta^2((1+C(x))^2-4B(x))}{4}\right)$$

est sans facteur carré (voir la proposition 4.4.1.2).

Soient $\beta\in\mathrm{Jac}(\mathcal{C}_\zeta^+)(k(x))$ et $\alpha:=\Pi_{\mathcal{C}_\zeta^+}(\beta)$. D'après la proposition 4.4.2.1, il existe

* un diviseur sans facteur carré $\mu_{1,3} \in k[x]$ de $1-2E=C$,
* un diviseur sans facteur carré $\mu_{1,4} \in k[x]$ de $(1-E)^2-D=B$,
* un diviseur sans facteur carré $\mu_{2,3} \in k[x]$ de

$$2E(E^2-D) = (1-C)(B-C), \text{ et}$$

* un diviseur sans facteur carré $\mu_{3,4} \in k[x]$ de $E^2-D=B-C$

tels que $\Xi_{\mathcal{C}_\zeta^+}(\beta) = ([\mu_{1,3}\mu_{1,4}], [\mu_{2,3}], [\mu_{1,3}\mu_{2,3}\mu_{3,4}], [\mu_{1,4}\mu_{3,4}])$. Les polynômes $\mu_{i,j}$ permettent aussi d'exprimer l'image $\Pi_{\mathcal{C}_\zeta^+}(\beta)$: nous avons

$$\alpha = \Pi_{\mathcal{C}_\zeta^+}(\beta) = \left([\mu_{1,3}\mu_{1,4}], [\mu_{1,3}\mu_{3,4}], [\mu_{1,4}\mu_{3,4}]\right).$$

Le polynôme C est irréductible. De plus, le polynôme B se factorise sous la forme

$$B = (x+b_1+\eta)(x+b_1-\eta)$$

et le polynôme $B-C$ se factorise sous la forme

$$B-C = (x+b_1-1+\omega)(x+b_1-1-\omega).$$

Ainsi, quitte à ajouter l'image par $\Xi_{\mathcal{C}_\zeta^+}$ d'un point de 2-torsion (ces images sont données par la proposition 4.4.1.3), nous pouvons supposer l'existence de trois éléments $\epsilon_{1,3}$, $\epsilon_{1,4}$, $\epsilon_{3,4} \in k^\times$ et deux entiers n_2, $n_3 \in \mathbb{N}$ tels que :

* $\mu_{1,3} = \epsilon_{1,3}$,
* $\mu_{1,4} = \epsilon_{1,4}(x+b_1+\eta)^{n_2}$ et
* $\mu_{3,4} = \epsilon_{3,4}(x+b_1-1+\omega)^{n_3}$.

Nous utilisons maintenant la proposition 4.4.3.4. Ses hypothèses sont bien vérifiées :

* les polynômes $(1-E)^2-D$ et $1-2E$ sont premiers entre eux et $E^2-D \equiv \Big((1-E)^2-D\Big) \bmod (1-2E)$, donc les polynômes E^2-D et $1-2E$ sont premiers entre eux ;
* les polynômes E et D sont premiers entre eux et $E^2-D \equiv -D \bmod E$, donc les polynômes E^2-D et E sont premiers entre eux ;
* le polynôme $E^2-D=B-C=(x+b_1-1)^2-\omega^2$ est sans facteur carré car $\omega \neq 0$ (en fait $|\omega| > 1+|\eta|$) ;
* les polynômes δ et E^2-D sont premiers entre eux (en fait $\delta = \zeta \in k^\times$ est une constante non nulle).

Le polynôme E^2-D se factorise sous la forme

$$E^2-D = B-C = (x+b_1-1-\omega)(x+b_1-1+\omega).$$

D'après la proposition 4.4.3.4, il existe deux entiers n_4, $n_6 \in \{0,1\}$ tels que

$$\begin{array}{l} \epsilon_{1,3}\epsilon_{1,4}(x+b_1+\eta)^{n_2} \sim \zeta^{n_3}(1-2E)^{n_4} \bmod (x+b_1-1+\omega) \text{ et} \\ \epsilon_{1,3}\epsilon_{1,4}(x+b_1+\eta)^{n_2} \sim (1-2E)^{n_6} \bmod (x+b_1-1-\omega). \end{array} \tag{4.24}$$

Nous utilisons alors les congruences

$$\begin{array}{rcl} x+b_1+\eta & \equiv & (1-\omega+\eta) \bmod (x+b_1-1+\omega) \\ x+b_1+\eta & \equiv & (1+\omega+\eta) \bmod (x+b_1-1-\omega) \end{array}$$

$$\begin{array}{rcl} 1-2E=C & = & 2\,(x+b_1)+\omega^2-\eta^2-1 \\ & \equiv & \left(\omega^2-\eta^2+1-2\omega\right) \bmod (x+b_1-1+\omega) \\ & \equiv & \left((\omega-1)^2-\eta^2\right) \bmod (x+b_1-1+\omega) \\ 1-2E=C & \equiv & \left((\omega+1)^2-\eta^2\right) \bmod (x+b_1-1-\omega) \end{array}$$

pour traduire les équivalences 4.24 sous la forme

$$\begin{array}{l} \epsilon_{1,3}\epsilon_{1,4}\,(1-\omega+\eta)^{n_2} \sim \zeta^{n_3}\left((\omega-1)^2-\eta^2\right)^{n_4} \text{ et} \\ \epsilon_{1,3}\epsilon_{1,4}\,(1+\omega+\eta)^{n_2} \sim \left((\omega+1)^2-\eta^2\right)^{n_6}. \end{array} \tag{4.25}$$

En multipliant ces deux équivalences, nous montrons finalement que

$$\left((\eta+1)^2-\omega^2\right)^{n_2} \sim \zeta^{n_3}\left((\omega-1)^2-\eta^2\right)^{n_4}\left((\omega+1)^2-\eta^2\right)^{n_6}. \tag{4.26}$$

Les éléments ζ, $(\omega-1)^2-\eta^2$ et $(\omega+1)^2-\eta^2$ sont strictement positifs, et $(\eta+1)^2-\omega^2$ est strictement négatif. Or deux éléments de $k^\times$ équivalents sous $\sim$ sont de même signe, donc l'équivalence 4.26 impose la parité de n_2. Par suite, les équivalences 4.25 imposent la positivité stricte de $\epsilon_{1,3}\epsilon_{1,4}$.

Les hypothèses de la proposition 4.4.3.2 sont vérifiées :

* le polynôme $E=\frac{1-C}{2}$ est sans facteur carré (il est de degré 1) ;
* les polynômes E et D sont premiers entre eux ;
* les polynômes E et $(1-E)^2-D$ sont premiers entre eux ;
* les polynômes $\delta=\zeta$ et E sont premiers entre eux (en fait $\delta=\zeta\in k^\times$ est une constante non nulle).

Nous utilisons la proposition 4.4.3.2 en remarquant la congruence $-\delta D\equiv\zeta(E^2-D) \bmod E$: nous avons

$$\mu_{1,3}\mu_{3,4}\sim 1 \bmod E \text{ ou } \mu_{1,3}\mu_{3,4}\sim\zeta(E^2-D) \bmod E.$$

Nous distinguons deux cas.

Lorsque $\mu_{3,4}=\epsilon_{3,4}\in k^\times$. Dans ce cas $n_3=0$ et l'équivalence 4.26 s'écrit

$$1\sim\left((\omega-1)^2-\eta^2\right)^{n_4}\left((\omega+1)^2-\eta^2\right)^{n_6}.$$

Par hypothèse, cette équivalence impose $n_4=n_6=0$. En particulier, les équivalences 4.25 signifient que $\epsilon_{1,3}\epsilon_{1,4}\sim 1$.

Nous appliquons alors la proposition 4.4.2.2 : comme D est de degré 1 et comme les polynômes $\mu_{1,4}$ et $\mu_{3,4}$ sont des constantes (car $n_2 = n_3 = 0$), nous avons

$$\mu_{1,4}\mu_{3,4} = \epsilon_{1,4}\epsilon_{3,4} \sim 1.$$

Finalement, nous avons

$$\mu_{1,4}\mu_{3,4} \sim 1 \text{ et } \mu_{1,3}\mu_{3,4} \sim 1,$$

c'est-à-dire $\alpha = ([1], [1], [1])$.

Lorsque $\mu_{3,4} = \epsilon_{3,4}\,(x + b_1 - 1 + \omega)$. Le polynôme $\mu_{1,4}$ est une constante et D est de degré 1 et de coefficient dominant $4\left(\omega^2 - \eta^2\right)$. Ainsi, d'après la proposition 4.4.2.2, nous avons

$$\mu_{1,4}\mu_{3,4} \sim -(\omega^2 - \eta^2)(x + b_1 - 1 + \omega).$$

Le reste de la division euclidienne du polynôme $x + b_1 - 1 + \omega$ par $-2E = C - 1 = 2(x + b_1 - 1) + \omega^2 - \eta^2$ est

$$-\frac{\omega^2 - \eta^2}{2} + \omega,$$

et le reste de la division euclidienne de

$$E^2 - D = B - C = (x + b_1 - 1)^2 - \omega^2$$

par $-2E = C - 1 = 2(x + b_1 - 1) + \omega^2 - \eta^2$ est

$$\frac{(\omega^2 - \eta^2)^2 - 4\omega^2}{4}.$$

Les deux équivalences

$$\mu_{1,3}\mu_{3,4} \sim 1 \bmod E \text{ ou } \mu_{1,3}\mu_{3,4} \sim \zeta(E^2 - D) \bmod E$$

se reformulent donc respectivement sous la forme

$$\begin{array}{l} \epsilon_{1,3}\epsilon_{3,4} \sim -2\left(\omega^2 - \eta^2 - 2\omega\right) \text{ ou} \\ \epsilon_{1,3}\epsilon_{3,4} \sim -2\zeta\left(\omega^2 - \eta^2 + 2\omega\right). \end{array}$$

Nous avons de plus l'équivalence $\epsilon_{1,4}\epsilon_{3,4} \sim -(\omega^2 - \eta^2)$. Ainsi, en utilisant les équivalences 4.25 et l'équivalence

$$\left(\epsilon_{1,3}\epsilon_{1,4}\right)\left(\epsilon_{1,3}\epsilon_{3,4}\right)\left(\epsilon_{1,4}\epsilon_{3,4}\right) \sim 1,$$

nous obtenons

$$\begin{array}{l} 2\left(\omega^2 - \eta^2\right)\left(\omega^2 - \eta^2 - 2\omega\right)\left(\left(\omega + 1\right)^2 - \eta^2\right)^{n_6} \sim 1 \text{ ou} \\ 2\left(\omega^2 - \eta^2\right)\left(\omega^2 - \eta^2 + 2\omega\right)\left(\left(\omega - 1\right)^2 - \eta^2\right)^{n_4} \sim 1. \end{array}$$

Aucune de ces équivalences n'est possible par hypothèse : le cas $\mu_{3,4} = \epsilon_{3,4}\,(x + b_1 - 1 + \omega)$ est impossible.

Proposition 4.4.4.2 *Soient η, ω, $\rho \in \mathbb{R}$ des réels. Soit $k := \mathbb{Q}(\eta, \omega, \rho)$. Nous posons :*

$$b_1 = \frac{\rho^2 - \eta^2}{\omega^2 - \eta^2} + \frac{\eta^2 - \omega^2}{4}.$$

Soient $B(x) := (x + b_1)^2 - \eta^2$ et $C(x) := 2(x + b_1) + \omega^2 - \eta^2 - 1$. Nous supposons que les éléments

* $\left(\omega^2 - \eta^2 - 1\right)^2 - 4\eta^2$ *et*
* $\left(\omega^2 - \eta^2 - 2\right)^2 - 4\eta^2$

sont non nuls.

À tout $\delta \in k(x)^\times$, nous associons la $k(x)$-courbe hyperelliptique $\mathcal{C}_\delta^+$ d'équation affine :

$$\mathcal{C}_\delta^+ : z^2 = \left(y + \tfrac{\delta(1+C(x))}{2}\right)\left(y^2 - \tfrac{\delta^2(1-C(x))^2}{4}\right)\left(y^2 - \tfrac{\delta^2((1+C(x))^2-4B(x))}{4}\right).$$

Nous supposons que $\omega > |\eta| + 1$, $\omega^2 - \eta^2 > 2\omega$, $b_1 > 1 + \frac{\omega^2-\eta^2}{2}$, et qu'aucun des éléments

* $\left((b_1 - 1)^2 - \omega^2\right)^{n_1}\left((\omega - 1)^2 - \eta^2\right)^{n_2}\left((\omega + 1)^2 - \eta^2\right)^{n_3}$ *(avec (n_1, n_2, n_3) un triplet non nul d'éléments de $\{0, 1\}$),*
* $2\left(\omega^2 - \eta^2\right)\left(2b_1 - 2 + \omega^2 - \eta^2\right)$,
* $2^{n_1}\left(\omega^2 - \eta^2 + 2\omega\right)(b_1 - 1 + \omega)\left(\omega^2 - \eta^2\right)^{n_1}\left(2b_1 - 2 + \omega^2 - \eta^2\right)^{1-n_1}$ $\times (\omega - 1 - \eta)^{1-n_2}(\omega - 1 + \eta)^{n_2}$ *(avec n_1, $n_2 \in \mathbb{N}$), et*
* $2^{1-n_1}\left(\omega^2 - \eta^2 + 2\omega\right)\left(\omega^2 - \eta^2\right)^{n_1}\left(2b_1 - 2 + \omega^2 - \eta^2\right)^{n_1}$ $\times (\omega - 1 - \eta)^{1-n_2}(\omega - 1 + \eta)^{n_2}$ *(avec n_1, $n_2 \in \mathbb{N}$)*

n'est un carré dans k.

Alors, pour tout $\zeta \in k^\times$ strictement positif, l'image de $\Pi_{\mathcal{C}^+_{\zeta x}}$ est engendrée par l'image des points de torsion 2-primaire de $Jac(\mathcal{C}^+_{\zeta x})(k(x))$.

Démonstration.

Soit $\zeta \in k^\times$ strictement positif. Nous allons utiliser lors de cette démonstration les propositions 4.4.2.1, 4.4.2.2, 4.4.3.2 et 4.4.3.4 en posant $\delta := \zeta x$, $E(x) := \frac{1-C(x)}{2}$ et $D = \frac{(1+C(x))^2-4B(x)}{4}$. Avec ces notations, nous avons :

* $1 - E = \frac{1+C}{2}$,
* $1 - 2E = C$,
* $E^2 - D = B - C$ et
* $(1 - E)^2 - D = B$.

Nous commençons par montrer quatre relations de primalité relative.

a. Le reste de la division euclidienne de

$$(1-E)^2 - D = B = (x+b_1)^2 - \eta^2$$

par $1-2E = C = 2(x+b_1) + \omega^2 - \eta^2 - 1$ est égal à

$$\frac{(\omega^2-\eta^2-1)^2 - 4\eta^2}{4} = \frac{(\omega^2-\eta^2-1-2\eta)(\omega^2-\eta^2-1+2\eta)}{4}.$$

Ce reste est non nul par hypothèse, donc les polynômes $1-2E = C$ et $(1-E)^2 - D = B$ sont premiers entre eux.

b. De même le reste

$$\frac{\left(\omega^2-\eta^2-2\right)^2 - 4\eta^2}{4} = \frac{(\omega^2-\eta^2-2-2\eta)(\omega^2-\eta^2-2+2\eta)}{4}$$

de la division euclidienne de $(1-E)^2 - D = B = (x+b_1)^2 - \eta^2$ par $E = \frac{1-C}{2} = -x - b_1 + 1 - \frac{\omega^2-\eta^2}{2}$ est non nul, donc les polynômes $(1-E)^2 - D = B$ et $E = \frac{1-C}{2}$ sont premiers entre eux.

c. Le reste de la division euclidienne de

$$4D = (1+C)^2 - 4B = 4(\omega^2-\eta^2)(x+b_1) + (\omega^2-\eta^2)^2 + 4\eta^2$$

par $1-2E = C = 2(x+b_1) + \omega^2 - \eta^2 - 1$ est égal à

$$-2(\omega^2-\eta^2)(\omega^2-\eta^2-1) + (\omega^2-\eta^2)^2 + 4\eta^2 = -\left(\omega^2-\eta^2\right)^2 + 2\omega^2 + 2\eta^2.$$

Ce reste est non nul : de l'inégalité $\omega^2 - \eta^2 > 2|\omega|$ nous déduisons

$$\left(\omega^2-\eta^2\right)^2 - 2\omega^2 - 2\eta^2 > 4\omega^2 - 2\omega^2 - 2\eta^2 = 2\left(\omega^2-\eta^2\right) > 0.$$

Les polynômes D et $1-2E$ sont donc premiers entre eux.

d. Enfin, le reste

$$-2(\omega^2-\eta^2)(\omega^2-\eta^2-2) + (\omega^2-\eta^2)^2 + 4\eta^2 = 4\omega^2 - (\omega^2-\eta^2)^2$$

de la division euclidienne de

$$\begin{aligned} 4D &= (1+C)^2 - 4B \\ &= 4\left(\omega^2-\eta^2\right)(x+b_1) + \left(\omega^2-\eta^2\right)^2 + 4\eta^2 \end{aligned}$$

par $E = \frac{1-C}{2} = -x-b_1+1-\frac{\omega^2-\eta^2}{2}$ est non nul (il est même strictement négatif : nous avons supposé $\omega^2 - \eta^2 > 2|\omega|$). Les polynômes D et E sont donc premiers entre eux.

Par ailleurs $\omega^2 > \eta^2$ (en fait $\omega^2 - \eta^2 > 2|\omega|$), donc le polynôme

$$\begin{aligned} 4D &= (1+C)^2 - 4B \\ &= 4\left(\omega^2-\eta^2\right)(x+b_1) + \left(\omega^2-\eta^2\right)^2 + 4\eta^2 \end{aligned}$$

est de degré 1. Par conséquent, le polynôme D n'est pas un carré dans $k(x)$. Les hypothèses de la proposition 4.4.2.1 sont donc vérifiées.

En particulier, les polynômes $(1-E)^2-D$, E, $1-2E$, D et E^2-D sont non nuls. Or $\delta=\zeta x$ est non nul (car ζ est non nul), donc le polynôme

$$\left(y+\tfrac{\delta(1+C(x))}{2}\right)\left(y-\tfrac{\delta(1-C(x))}{2}\right)\left(y+\tfrac{\delta(1-C(x))}{2}\right)\left(y^2-\tfrac{\delta^2((1+C(x))^2-4B(x))}{4}\right)$$

est sans facteur carré (voir la proposition 4.4.1.2).

Soient $\beta\in\mathrm{Jac}(\mathcal{C}^+_{\zeta x})(k(x))$ et $\alpha:=\Pi_{\mathcal{C}^+_{\zeta x}}(\beta)$. D'après la proposition 4.4.2.1, il existe

* un diviseur sans facteur carré $\mu_{1,3}\in k[x]$ de $\delta(1-2E)=\zeta xC$,
* un diviseur sans facteur carré $\mu_{1,4}\in k[x]$ de $\delta\left((1-E)^2-D\right)=\zeta xB$,
* un diviseur sans facteur carré $\mu_{2,3}\in k[x]$ de

$$2\delta E(E^2-D)=\zeta x(1-C)(B-C),\text{ et}$$

* un diviseur sans facteur carré $\mu_{3,4}\in k[x]$ de $\delta\left(E^2-D\right)=\zeta x(B-C)$

tels que $\Xi_{\mathcal{C}^+_{\zeta x}}(\beta)=([\mu_{1,3}\mu_{1,4}],[\mu_{2,3}],[\mu_{1,3}\mu_{2,3}\mu_{3,4}],[\mu_{1,4}\mu_{3,4}])$. Les polynômes $\mu_{i,j}$ permettent aussi d'exprimer l'image $\Pi_{\mathcal{C}^+_{\zeta x}}(\beta)$: nous avons

$$\alpha=\Pi_{\mathcal{C}^+_{\zeta x}}(\beta)=\left([\mu_{1,3}\mu_{1,4}],[\mu_{1,3}\mu_{3,4}],[\mu_{1,4}\mu_{3,4}]\right).$$

Puisque $\Xi_{\mathcal{C}^+_{\zeta x}}(\beta)=([(x\mu_{1,3})(x\mu_{1,4})],[\mu_{2,3}],[(x\mu_{1,3})\mu_{2,3}(x\mu_{3,4})],[(x\mu_{1,4})(x\mu_{3,4})])$, nous pouvons supposer, quitte à remplacer $\mu_{1,3}$, $\mu_{1,4}$ et $\mu_{3,4}$ respectivement par les versions sans facteur carré de $x\mu_{1,3}$, $x\mu_{1,4}$ et $x\mu_{3,4}$, que la valuation en x de $\mu_{1,4}$ est nulle.

Le polynôme $B=(1-E)^2-D$ se factorise sous la forme

$$B=(x+b_1+\eta)(x+b_1-\eta)$$

et le polynôme $C=1-2E$ est de degré 1. Quitte à ajouter l'image par $\Xi_{\mathcal{C}^+_{\zeta x}}$ d'un point de 2-torsion (voir la proposition 4.4.1.3), nous pouvons donc supposer, sans perte de généralité, l'existence de deux éléments $\epsilon_{1,3}\in k^\times$ et $\epsilon_{1,4}\in k^\times$ et un entier $n_1\in\mathbb{N}$ tels que :

* $\mu_{1,3}=\epsilon_{1,3}$, et
* $\mu_{1,4}=\epsilon_{1,4}(x+b_1+\eta)^{n_1}$

Nous utilisons maintenant la proposition 4.4.3.4. Ses hypothèses sont bien vérifiées :

* les polynômes $(1-E)^2-D$ et $1-2E$ sont premiers entre eux et $E^2-D\equiv\left((1-E)^2-D\right)\bmod(1-2E)$, donc les polynômes E^2-D et $1-2E$ sont premiers entre eux ;
* les polynômes E et D sont premiers entre eux et $E^2-D\equiv -D\bmod E$, donc les polynômes E^2-D et E sont premiers entre eux ;

* le polynôme $E^2 - D = B - C = (x + b_1 - 1)^2 - \omega^2$ est sans facteur carré car $\omega \neq 0$ (en fait $\omega > 1 + |\eta|$) ;
* les polynômes $\delta = \zeta x$ et $E^2 - D$ sont premiers entre eux car

$$E(0)^2 - D(0) = B(0) - C(0) = (b_1 - 1)^2 - \omega^2 > 0$$

(nous avons $b_1 - 1 > \frac{\omega^2 - \eta^2}{2}$ et $\omega^2 - \eta^2 > 2|\omega|$).

Nous notons respectivement n_2 et n_4 les valuations en $x + b_1 - 1 + \omega$ et $x + b_1 - 1 - \omega$ du polynôme $\mu_{3,4}$. D'après la proposition 4.4.3.4, il existe deux entiers n_3, $n_5 \in \{0, 1\}$ tels que

$$\begin{array}{l} \epsilon_{1,3}\epsilon_{1,4}\,(x + b_1 + \eta)^{n_1} \sim \delta^{n_2}(1 - 2E)^{n_3} \bmod (x + b_1 - 1 + \omega) \text{ et} \\ \epsilon_{1,3}\epsilon_{1,4}\,(x + b_1 + \eta)^{n_1} \sim \delta^{n_4}(1 - 2E)^{n_5} \bmod (x + b_1 - 1 - \omega)\,. \end{array} \tag{4.27}$$

Nous utilisons alors les congruences

$$\begin{array}{rcl} x + b_1 + \eta & \equiv & (1 - \omega + \eta) \bmod (x + b_1 - 1 + \omega) \\ x + b_1 + \eta & \equiv & (1 + \omega + \eta) \bmod (x + b_1 - 1 - \omega) \end{array}$$

$$\begin{array}{rcl} 1 - 2E = C & = & 2\,(x + b_1) + \omega^2 - \eta^2 - 1 \\ & \equiv & \left(\omega^2 - \eta^2 + 1 - 2\omega\right) \bmod (x + b_1 - 1 + \omega) \\ & \equiv & \left((\omega - 1)^2 - \eta^2\right) \bmod (x + b_1 - 1 + \omega) \\ 1 - 2E = C & \equiv & \left((\omega + 1)^2 - \eta^2\right) \bmod (x + b_1 - 1 - \omega) \end{array}$$

$$\begin{array}{rcl} x & \equiv & (1 - \omega - b_1) \bmod (x + b_1 - 1 + \omega) \\ x & \equiv & (1 + \omega - b_1) \bmod (x + b_1 - 1 - \omega) \end{array}$$

pour traduire les équivalences 4.27 sous la forme

$$\begin{array}{l} \epsilon_{1,3}\epsilon_{1,4}\,(1 - \omega + \eta)^{n_1} \sim \zeta^{n_2}\,(1 - \omega - b_1)^{n_2}\left((\omega - 1)^2 - \eta^2\right)^{n_3} \text{ et} \\ \epsilon_{1,3}\epsilon_{1,4}\,(1 + \omega + \eta)^{n_1} \sim \zeta^{n_4}\,(1 + \omega - b_1)^{n_4}\left((\omega + 1)^2 - \eta^2\right)^{n_5}. \end{array} \tag{4.28}$$

En multipliant ces deux équivalences, nous montrons finalement que

$$\begin{array}{rcl} \left((\eta + 1)^2 - \omega^2\right)^{n_1} & \sim & \zeta^{n_2 + n_4}\,(1 - \omega - b_1)^{n_2}\,(1 + \omega - b_1)^{n_4} \\ & & \times \left((\omega - 1)^2 - \eta^2\right)^{n_3}\left((\omega + 1)^2 - \eta^2\right)^{n_5}. \end{array} \tag{4.29}$$

Par ailleurs, les éléments

* ζ, $(\omega - 1)^2 - \eta^2$ et $(\omega + 1)^2 - \eta^2$ sont strictement positifs ;
* $(\eta + 1)^2 - \omega^2$, $1 - \omega - b_1 = -\frac{\omega^2 - \eta^2 + 2\omega}{2} - \left(b_1 - 1 - \frac{\omega^2 - \eta^2}{2}\right)$ et $1 + \omega - b_1 = -\frac{\omega^2 - \eta^2 - 2\omega}{2} - \left(b_1 - 1 - \frac{\omega^2 - \eta^2}{2}\right)$ sont strictement négatifs.

Or deux éléments de $k^\times$ équivalents sous $\sim$ sont de même signe, donc l'équivalence 4.29 n'est possible que dans le cas où l'entier $n_1 + n_2 + n_4$ est pair.

Dans ce qui suit nous utilisons la proposition 4.4.3.2. Les hypothèses de cette proposition sont vérifiées :

* le polynôme $E = \frac{1-C}{2}$ est sans facteur carré (il est de degré 1) ;
* les polynômes E et D sont premiers entre eux ;
* les polynômes E et $(1-E)^2 - D$ sont premiers entre eux ;
* les polynômes $\delta = \zeta x$ et E sont premiers entre eux (car $E(0) = \frac{1-C(0)}{2} = 1 - b_1 - \frac{\omega^2-\eta^2}{2} < 0$).

Lorsque $\mu_{1,4} = \epsilon_{1,4} \in k^\times$. Alors n_1 est nul et donc n_2 et n_4 sont de même parité. L'équivalence 4.29 s'écrit alors

$$1 \sim \left((b_1-1)^2 - \omega^2\right)^{n_2} \left((\omega-1)^2 - \eta^2\right)^{n_3} \left((\omega+1)^2 - \eta^2\right)^{n_5}.$$

Par hypothèse, cette équivalence impose $n_2 = n_3 = n_5 = 0$. L'équivalence 4.28 s'écrit donc $\epsilon_{1,3}\epsilon_{1,4} \sim 1$. De plus, comme $n_2 = n_4 = 0$, il existe une constante non nulle $\epsilon_{3,4} \in k^\times$ telle que $\mu_{3,4} = \epsilon_{3,4} x^{v_x(\mu_{3,4})}$ (car $\mu_{3,4}$ est sans facteur carré).

Nous distinguons deux sous-cas.

Lorsque $v_x(\mu_{3,4}) = 0$. Alors, les polynômes $\mu_{1,4}$ et $\mu_{3,4}$ sont des éléments de $k^\times$. De plus, le polynôme D est de degré 1. Ainsi, d'après la proposition 4.4.2.2, nous avons $\mu_{1,4}\mu_{3,4} \sim 1$.

Or les équivalences 4.28 signifient que $\mu_{1,3}\mu_{1,4} \sim 1$, donc l'élément $\alpha = ([\mu_{1,3}\mu_{1,4}], [\mu_{1,3}\mu_{3,4}], [\mu_{1,4}\mu_{3,4}]) = ([1],[1],[1])$ est la classe triviale.

Lorsque $v_x(\mu_{3,4}) = 1$. Alors, le polynôme $\mu_{1,4}\mu_{3,4}$ est le produit de x par un élément de $k^\times$. Ainsi, d'après la proposition 4.4.2.2, nous avons $\mu_{1,4}\mu_{3,4} \sim -(\omega^2 - \eta^2)x$.

Nous faisons maintenant appel à la proposition 4.4.3.2 : nous avons

$$\mu_{1,3}\mu_{3,4} \sim 1 \bmod E \text{ ou } \mu_{1,3}\mu_{3,4} \sim \zeta x(E^2 - D) \bmod E,$$

c'est-à-dire (puisque $\mu_{1,3}\mu_{1,4} \sim 1$ et $\mu_{1,4}\mu_{3,4} \sim -(\omega^2-\eta^2)x$)

$$-(\omega^2-\eta^2)x \sim 1 \bmod E \text{ ou } -(\omega^2-\eta^2)(E^2-D) \sim \zeta \bmod E.$$

Le reste de la division euclidienne de

$$E^2 - D = B - C = (x + b_1 - 1)^2 - \omega^2$$

par $-2E = C - 1 = 2(x + b_1 - 1) + \omega^2 - \eta^2$ est

$$\frac{(\omega^2 - \eta^2)^2 - 4\omega^2}{4} = \frac{(\omega^2 - \eta^2 - 2\omega)(\omega^2 - \eta^2 + 2\omega)}{4}.$$

Ce reste est strictement positif. Deux éléments de $k^\times$ équivalents sous $\sim$ sont de même signe. Or $-(\omega^2 - \eta^2) < 0$ et $\zeta > 0$, donc l'équivalence

$$-(\omega^2 - \eta^2)(E^2 - D) \sim \zeta \bmod E$$

n'est pas possible.

Le reste de la division euclidienne de x par

$$-2E = 2(x + b_1 - 1) + \omega^2 - \eta^2$$

est $-\left(b_1 - 1 + \frac{\omega^2 - \eta^2}{2}\right)$. L'équivalence $-(\omega^2 - \eta^2)x \sim 1 \bmod E$ se réécrit donc

$$2\left(\omega^2 - \eta^2\right)\left(2b_1 - 2 + \omega^2 - \eta^2\right) \sim 1.$$

Cette équivalence est en contradiction avec les hypothèses, donc $v_x(\mu_{3,4}) = 0$.

Lorsque $\mu_{1,4} = \epsilon_{1,4}(x + b_1 + \eta)$. Alors les entiers n_2 et n_4 sont de parités différentes. Nous allons distinguer deux cas suivant les parités de n_2 et n_4.

Lorsque n_2 est impair. Alors n_4 est pair. Ainsi, le polynôme $\mu_{3,4}$ étant sans facteur carré, il existe une constante non nulle $\epsilon_{3,4} \in k^\times$ et un entier $n_6 \in \{0, 1\}$ tels que $\mu_{3,4} = \epsilon_{3,4} x^{n_6}(x + b_1 - 1 + \omega)$.

Nous faisons maintenant appel à la proposition 4.4.3.2 : nous avons

$$\mu_{1,3}\mu_{3,4} \sim 1 \bmod E \text{ ou } \mu_{1,3}\mu_{3,4} \sim \zeta x\left(E^2 - D\right) \bmod E,$$

Nous reformulons ces deux équivalences en utilisant les égalités

$$\begin{array}{l}\mu_{1,3}\mu_{3,4} = \epsilon_{1,3}\epsilon_{3,4} x^{n_6}(x + b_1 - 1 + \omega), \text{ et} \\ E^2 - D = B - C = (x + b_1 - 1 + \omega)(x + b_1 - 1 - \omega).\end{array}$$

Nous obtenons

$$\begin{array}{l}\epsilon_{1,3}\epsilon_{3,4} x^{n_6}(x + b_1 - 1 + \omega) \sim 1 \bmod E \text{ ou} \\ \epsilon_{1,3}\epsilon_{3,4} x^{1-n_6}(x + b_1 - 1 - \omega) \sim \zeta \bmod E.\end{array} \tag{4.30}$$

Nous utilisons la proposition 4.4.2.2 : le coefficient dominant du polynôme $\mu_{1,4}\mu_{3,4} = \epsilon_{1,4}\epsilon_{3,4} x^{n_6}(x + b_1 + \eta)(x + b_1 - 1 + \omega)$ vérifie l'équivalence

$$\epsilon_{1,4}\epsilon_{3,4} \sim \left(-(\omega^2 - \eta^2)\right)^{n_6}.$$

Ce coefficient dominant est du signe de $(-1)^{n_6}$. Or $\epsilon_{1,3}\epsilon_{1,4}$ est strictement positif (nous nous en apercevons en utilisant les équivalences 4.28, la parité de n_4 et la positivité stricte des éléments ζ, $1+\omega+\eta$ et $(\omega+1)^2-\eta^2$), donc le coefficient $\epsilon_{1,3}\epsilon_{3,4}$ est du signe de $(-1)^{n_6}$.

Par ailleurs, le reste $-\left(b_1-1+\frac{\omega^2-\eta^2}{2}\right)$ de la division euclidienne de x par

$$-2E = C-1 = 2\left(x+b_1-1\right)+\omega^2-\eta^2,$$

le reste $-\frac{\omega^2-\eta^2-2\omega}{2}$ de la division euclidienne de $x+b_1-1+\omega$ par $-2E=C-1$ et le reste $-\frac{\omega^2-\eta^2+2\omega}{2}$ de la division euclidienne de $x+b_1-1-\omega$ par $-2E=C-1$ sont strictement négatifs.

Ainsi, deux éléments de $k^\times$ équivalents sous $\sim$ étant de même signe, la seule équivalence possible parmi les équivalences 4.30 est

$$\epsilon_{1,3}\epsilon_{3,4}x^{1-n_6}(x+b_1-1-\omega)\sim\zeta \bmod E,$$

c'est-à-dire

$$(-2)^{n_6}\epsilon_{1,3}\epsilon_{3,4}\left(2b_1-2+\omega^2-\eta^2\right)^{1-n_6}\left(\omega^2-\eta^2+2\omega\right)\sim\zeta.$$

Pour conclure nous utilisons les deux équivalences

$$\begin{array}{l}\epsilon_{1,4}\epsilon_{3,4}\sim\left(-(\omega^2-\eta^2)\right)^{n_6}\text{ et}\\ \epsilon_{1,3}\epsilon_{1,4}\sim\zeta\left(b_1-1+\omega\right)\left(\omega-1-\eta\right)^{1-n_3}\left(\omega-1+\eta\right)^{n_3}\end{array}$$

(la seconde équivalence est une des deux équivalences 4.28). Nous montrons ainsi

$$\begin{array}{rcl}1&\sim&2^{n_6}\left(\omega^2-\eta^2+2\omega\right)\left(b_1-1+\omega\right)\left(\omega^2-\eta^2\right)^{n_6}\times\\&&\left(2b_1-2+\omega^2-\eta^2\right)^{1-n_6}\left(\omega-1-\eta\right)^{1-n_3}\left(\omega-1+\eta\right)^{n_3},\end{array}$$

ce qui contredit les hypothèses.

Lorsque n_2 est pair. Alors n_4 est impair. Ainsi, le polynôme $\mu_{3,4}$ étant sans facteur carré, il existe une constante non nulle $\epsilon_{3,4}\in k^\times$ et un entier $n_6\in\{0,1\}$ tels que $\mu_{3,4}=\epsilon_{3,4}x^{n_6}(x+b_1-1-\omega)$.

Nous faisons maintenant appel à la proposition 4.4.3.2 : nous avons

$$\mu_{1,3}\mu_{3,4}\sim 1 \bmod E \text{ ou } \mu_{1,3}\mu_{3,4}\sim\zeta x\left(E^2-D\right) \bmod E,$$

Nous reformulons ces deux équivalences en utilisant les égalités

$$\begin{array}{l}\mu_{1,3}\mu_{3,4}=\epsilon_{1,3}\epsilon_{3,4}x^{n_6}(x+b_1-1-\omega),\text{ et}\\ E^2-D=B-C=\left(x+b_1-1+\omega\right)\left(x+b_1-1-\omega\right).\end{array}$$

Nous obtenons

$$\begin{array}{l}\epsilon_{1,3}\epsilon_{3,4}x^{n_6}(x+b_1-1-\omega)\sim 1 \bmod E \text{ ou}\\ \epsilon_{1,3}\epsilon_{3,4}x^{1-n_6}(x+b_1-1+\omega)\sim \zeta \bmod E.\end{array} \tag{4.31}$$

Nous utilisons la proposition 4.4.2.2 : le coefficient dominant du polynôme $\mu_{1,4}\mu_{3,4}=\epsilon_{1,4}\epsilon_{3,4}x^{n_6}(x+b_1+\eta)(x+b_1-1-\omega)$ vérifie l'équivalence

$$\epsilon_{1,4}\epsilon_{3,4}\sim\left(-(\omega^2-\eta^2)\right)^{n_6}.$$

Ce coefficient dominant est du signe de $(-1)^{n_6}$. Or $\epsilon_{1,3}\epsilon_{1,4}$ est strictement négatif (nous nous en apercevons en utilisant les équivalences 4.28, la parité de n_2 et la stricte positivité de $\omega-1-\eta$ et $(\omega-1)^2-\eta^2$), donc le coefficient $\epsilon_{1,3}\epsilon_{3,4}$ est du signe de $(-1)^{1-n_6}$. Par ailleurs, le reste $-\left(b_1-1+\frac{\omega^2-\eta^2}{2}\right)$ de la division euclidienne de x par

$$-2E=C-1=2\left(x+b_1-1\right)+\omega^2-\eta^2$$

le reste $-\frac{\omega^2-\eta^2-2\omega}{2}$ de la division euclidienne de $x+b_1-1+\omega$ par $-2E=C-1$ et le reste $-\frac{\omega^2-\eta^2+2\omega}{2}$ de la division euclidienne de $x+b_1-1-\omega$ par $-2E=C-1$ sont strictement négatifs. Ainsi, deux éléments de $k^\times$ équivalents sous $\sim$ étant de même signe, la seule équivalence possible parmi les équivalences 4.31 est

$$\epsilon_{1,3}\epsilon_{3,4}x^{n_6}(x+b_1-1-\omega)\sim 1 \bmod E,$$

c'est-à-dire

$$(-2)^{1-n_6}\epsilon_{1,3}\epsilon_{3,4}\left(2b_1-2+\omega^2-\eta^2\right)^{n_6}\left(\omega^2-\eta^2+2\omega\right)\sim 1.$$

Pour conclure nous utilisons les deux équivalences

$$\begin{array}{l}\epsilon_{1,4}\epsilon_{3,4}\sim\left(-(\omega^2-\eta^2)\right)^{n_6} \text{ et}\\ \epsilon_{1,3}\epsilon_{1,4}\sim-\left(\omega-1-\eta\right)^{1-n_3}\left(\omega-1+\eta\right)^{n_3}\end{array}$$

(la seconde équivalence est une des deux équivalences 4.28). Nous montrons ainsi

$$\begin{array}{rcl}1 & \sim & 2^{1-n_6}\left(\omega^2-\eta^2+2\omega\right)\left(\omega^2-\eta^2\right)^{n_6}\left(2b_1-2+\omega^2-\eta^2\right)^{n_6}\\ & & \times\left(\omega-1-\eta\right)^{1-n_3}\left(\omega-1+\eta\right)^{n_3},\end{array}$$

ce qui contredit les hypothèses.

Finalement, les deux cas précédents étant impossibles, l'entier n_1 doit être paire. □

4.5 Etude de l'image de $\Pi_{\widehat{\mathcal{C}}_\delta^+}$.

Soit k un sous-corps de $\mathbb{R}$. Soient B, C, $\delta \in k[x]$ trois polynômes. Nous considérons la courbe hyperelliptique $\mathcal{H}$ d'équation affine

$$\mathcal{H} : z^2 = (y + \delta(1 + C))(y^2 - 4\delta^2 B)(y^2 - 4\delta^2 C).$$

Notations 4.5.1 Nous notons
* $L_1(y) := y + \delta(1 + C)$,
* $L_2(y) := y^2 - 4\delta^2 B$ et
* $L_3(y) := y^2 - 4\delta^2 C$.

Nous supposons que le polynôme $L_1(y)L_2(y)L_3(y)$ est sans facteur carré, et que les polynômes B et C ne sont pas des carrés dans $k(x)$.

Pour tout $i \in \{1, 2, 3\}$ nous posons $K_i := k(x)[y]/(L_i(y))$ et nous notons y_i la classe de y dans K_i.

Soit $\pi_{\mathcal{H}} : \mathrm{Jac}(\mathcal{H})(k(x)) \longrightarrow \prod_{i=1}^{3} K_i^\times / K_i^{\times 2}$ le morphisme de Cassels-Schaefer et $\pi_{\mathcal{H},i} : \mathrm{Jac}(\mathcal{H})(k(x)) \longrightarrow K_i^\times / K_i^{\times 2}$ sa i-ème composante.

La norme $N_{K_i/k(x)}$ de l'extension $K_i/k(x)$ induit un homomorphisme $N_{K_i/k(x)} : K_i^\times / K_i^{\times 2} \longrightarrow k(x)^\times / k(x)^{\times 2}$. Nous posons $\Xi_{\mathcal{H},i} := N_{K_i/k(x)} \circ \pi_{\mathcal{H},i}$ et nous notons $\Xi_{\mathcal{H}} : \mathrm{Jac}(\mathcal{H})(k(x)) \longrightarrow \prod_{i=1}^{3} k(x)^\times / k(x)^{\times 2}$ l'homomorphisme de i-ème coordonnée $\Xi_{\mathcal{H},i}$.

Proposition 4.5.2 *Soit k un corps de caractéristique 0. Soient B, C, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1 - C$, $B - C$ et $(1 + C)^2 - 4B$ soient non nuls.*

Alors le polynôme $(y + \delta(1 + C))(y^2 - 4\delta^2 B)(y^2 - 4\delta^2 C)$ est sans facteur carré.

Démonstration.

Les polynômes B et C sont non nuls. Or $\delta \neq 0$, donc les polynômes $y^2 - 4\delta^2 B$ et $y^2 - 4\delta^2 C$ sont sans facteur carré.

Le polynôme $(1 + C)^2 - 4B$ est non nul. Les polynômes $y^2 - 4\delta^2 B$ et $y + \delta(1 + C)$ sont donc premiers entre eux.

De même, le polynôme $(1 + C)^2 - 4C = (1 - C)^2$ étant non nul, les polynômes $y^2 - 4\delta^2 C$ et $y + \delta(1 + C)$ sont premiers entre eux.

Le polynôme $B - C$ est non nul. Nous en déduisons que les polynômes $y^2 - 4\delta^2 B$ et $y^2 - 4\delta^2 C$ sont premiers entre eux. Ainsi le polynôme

$$(y + \delta(1 + C))(y^2 - 4\delta^2 B)(y^2 - 4\delta^2 C)$$

est sans facteur carré. □

Proposition 4.5.3 *Soit k un corps de caractéristique 0. Soient B, C, $\delta \in k[x]$ trois polynômes non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y + \delta(1 + C))(y^2 - 4\delta^2 B)(y^2 - 4\delta^2 C).$$

Nous reprenons les notations 4.5.1. Nous supposons que

* *B et C sont premiers entre eux, et*
* *B, C, $B - C$ et $(1 + C)^2 - 4B$ ne sont pas des carrés dans $k(x)$.*

Alors l'image par $\Xi_{\mathcal{H}}$ de la torsion de $Jac(\mathcal{H})(k(x))$ est l'image par $\Xi_{\mathcal{H}}$ de la 2-torsion de $Jac(\mathcal{H})(k(x))$. Elle est donc engendrée par la classe $\left([(1 + C)^2 - 4B], [(1 + C)^2 - 4B], [1]\right)$.

Démonstration.

Les polynômes B, C, $B-C$ et $(1+C)^2-4B$ ne sont pas des carrés dans $k(x)$. Par conséquent, ces quatre polynômes sont non nuls. Puisque C nest pas un carré dans $k(x)$, le polynôme $1 - C$ est non nul. Ainsi, nous sommes sous les hypothèses de la proposition 4.5.2.

Nous avons supposé que B et C ne sont pas des carrés dans $k(x)$ et que δ est non nul. Les polynômes $y^2 - 4\delta^2 B$ et $y^2 - 4\delta^2 C$ sont donc irréductibles. Ainsi, d'après la proposition 1.4.12, la 2-torsion de $\mathrm{Jac}(\mathcal{H})(k(x))$ est engendrée par les points

$$< y + \delta(1 + C), 0 > \text{ et } < y^2 - 4\delta^2 B, 0 > .$$

Puisque $y + \delta(1 - C)$ est premier aux polynômes $L_2(y) = y^2 - 4\delta^2 B$ et $L_3(y) = y^2 - 4\delta^2 B$, nous avons :

* $\Xi_{\mathcal{H},2}(< y+\delta(1+C), 0 >) = \left[\delta^2\left((1 + C)^2 - 4B\right)\right] = \left[(1 + C)^2 - 4B\right]$,
* et $\Xi_{\mathcal{H},3}(< y + \delta(1 + C), 0 >) = \left[\delta^2(1 - C)^2\right] = [1]$.

Les composantes de $\Xi_{\mathcal{H}}$ sont toutes à valeurs dans $k(x)^\times/k(x)^{\times 2}$. D'après la proposition 1.5.9, leur produit est l'élément trivial de $k(x)^\times/k(x)^{\times 2}$. En particulier, l'image $\Xi_{\mathcal{H}}(< y + \delta(1 + C), 0 >)$ est égale à la classe

$$([(1 + C)^2 - 4B], [(1 + C)^2 - 4B], [1]).$$

De même, nous montrons que

$$\Xi_{\mathcal{H}}(< y^2 - 4\delta^2 B, 0 >) = ([(1 + C)^2 - 4B], [(1 + C)^2 - 4B], [1]).$$

Nous avons supposé que $(1+C)^2-4B$ n'est pas un carré dans $k(x)$. Les images de $< y + \delta(1 + C), 0 >$ et $< y^2 - 4\delta^2 B, 0 >$ par $\Xi_{\mathcal{H}}$ ne sont donc pas triviales. Or L'image d'un double de $\mathrm{Jac}(\mathcal{H})(k(x))$ par $\Xi_{\mathcal{H}}$ est triviale. Les points $< y + \delta(1 + C), 0 >$ et $< y^2 - 4\delta^2 B, 0 >$ n'appartiennent donc pas à $2\mathrm{Jac}(\mathcal{H})(k(x))$.

Les polynômes B et $B-C$ sont premiers entre eux et $B-C$ n'est pas un carré dans $k(x)$. En utilisant la décomposition en facteurs premiers dans $k(x)$, nous en déduisons que $B-C$ et $B(B-C)$ ne sont pas des carrés dans $k(x)$. Ainsi, d'après la proposition 2.3.2.1, $B-C$ n'est pas un carré dans K_2. Cela signifie que l'image par $\pi_{\mathcal{H},2}$ du point $< y^2-4\delta^2 C, 0 >$ n'est pas triviale. Par conséquent, le point

$$< y^2-4\delta^2 C, 0 >=< y+\delta(1+C), 0 > + < y^2-4\delta^2 B, 0 >$$

n'est pas un double dans $\mathrm{Jac}(\mathcal{H})(k(x))$.

Finalement la 4-torsion de $\mathrm{Jac}(\mathcal{H})(k(x))$ est égale à sa 2-torsion. Nous en déduisons que la torsion 2-primaire de $\mathrm{Jac}(\mathcal{H})(k(x))$ est aussi égale à sa 2-torsion.

Comme l'image d'un double par $\Xi_{\mathcal{H}}$ est triviale, nous avons, pour tout entier $m \in \mathbb{N}$ impair, l'égalité $\Xi_{\mathcal{H}}(T) = \Xi_{\mathcal{H}}(mT)$. En particulier, pour tout $m \in \mathbb{N}$ impair, tout $n \in \mathbb{N}$ et tout point de $2^n m$-torsion T, l'image $\Xi_{\mathcal{H}}(T)$ est l'image du point de 2^n-torsion mT par $\Xi_{\mathcal{H}}$. Ainsi, l'image de la torsion de $\mathrm{Jac}(\mathcal{H})(k(x))$ par $\Xi_{\mathcal{H}}$ est l'image de la torsion 2-primaire, c'est-à-dire l'image de la 2-torsion. □

Proposition 4.5.4 *Soit k un corps de caractéristique 0. Soient B, C, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-C$, $B-C$ et $(1+C)^2-4B$ soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y+\delta(1+C))(y^2-4\delta^2 B)(y^2-4\delta^2 C).$$

Nous reprenons les notations 4.5.1. Nous supposons que

* *B et C ne sont pas des carrés dans $k(x)$,*
* *B et C sont premiers entre eux,*
* *B et $C-1$ sont premiers entre eux,*
* *$(1+C)^2-4B$ et C sont premiers entre eux, et*
* *$B-1$ et $1-C$ sont premiers entre eux.*

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\mu_{1,2}\mu_{1,3}], [\mu_{1,2}\mu_{2,3}], [\mu_{1,3}\mu_{2,3}]) \text{ avec}$$

* *$\mu_{1,2} \in k[x]$ un diviseur de $\delta((1+C)^2-4B)$,*
* *$\mu_{1,3} \in k[x]$ un diviseur de $\delta(1-C)$ et*
* *$\mu_{2,3} \in k[x]$ un diviseur de $\delta(B-C)$.*

Démonstration.

Nous utilisons la proposition 4.1.3. Cela, nous amène à considérer les six polynômes suivants :

* $\Delta_{1,1} = N_{K_1/k(x)}(1) = 1$,

* $\Delta_{1,2} = N_{K_1/k(x)}\left(y^2 - 4\delta^2 B\right) = \delta^2\left((1+C)^2 - 4B\right)$,
* $\Delta_{1,3} = N_{K_1/k(x)}\left(y^2 - 4\delta^2 C\right) = \delta^2(1-C)^2$,
* $\Delta_{2,2} = N_{K_2/k(x)}(2y) = -16\delta^2 B$,
* $\Delta_{2,3} = N_{K_2/k(x)}\left(y^2 - 4\delta^2 C\right) = 16\delta^4(B-C)^2$ et
* $\Delta_{3,3} = N_{K_3/k(x)}(2y) = -16\delta^2 C$.

Lorsque $1 \leq j < i \leq 3$ nous posons également $\Delta_{j,i} := \Delta_{i,j}$.

Soit α un élément de l'image de $\Xi_{\mathcal{H}}$. D'après la proposition 4.1.3, il existe une famille $(\mu_{i,j})_{\substack{1 \leq i \leq 3,\\ j \neq i}}$ d'éléments de $k[x]$ sans facteur carré telle que

* $\mu_{i,j}$ divise $\operatorname{pgcd}\left(\prod_{k=1}^{3} \Delta_{i,k}, \prod_{l=1}^{3} \Delta_{j,l}\right)$,
* $\mu_{i,j} = \mu_{j,i}$, et
* $\Xi_{\mathcal{H},i}(\alpha)$ soit la classe de $\prod_{j \neq i} \mu_{i,j}$.

1. Le polynôme $\mu_{1,2}$ divise

$$\operatorname{pgcd}\left(\delta^4\left((1+C)^2 - 4B\right)(1-C)^2, -(16)^2\delta^8\left((1+C)^2 - 4B\right)B(B-C)^2\right).$$

Puisque $1-C$ et $1-B$ sont premiers entre eux, nous avons

$$\operatorname{pgcd}(B-C, (1-C)^2) = 1.$$

Les polynômes B et $1-C$ sont aussi premiers entre eux. Ainsi, le polynôme $\mu_{1,2}$ étant sans facteur carré, il divise $\delta\left((1+C)^2 - 4B\right)$.

2. Le polynôme $\mu_{1,3}$ divise

$$\operatorname{pgcd}\left(\delta^4\left((1+C)^2 - 4B\right)(1-C)^2, -(16)^2\delta^8(1-C)^2(B-C)^2C\right).$$

Les polynômes $1-C$ et $1-B$ sont premiers entre eux et

$$\operatorname{pgcd}(B-C, (1+C)^2 - 4B) = \operatorname{pgcd}(B-C, (1-C)^2),$$

donc les polynômes $B-C$ et $(1+C)^2 - 4B$ sont premiers entre eux. Or les polynômes $(1+C)^2 - 4B$ et C sont premiers entre eux et $\mu_{1,3}$ est sans facteur carré, donc $\mu_{1,3}$ divise $\delta(1-C)$.

3. Le polynôme $\mu_{2,3}$ divise

$$\operatorname{pgcd}\left(-16\delta^8\left((1+C)^2 - 4B\right)B(B-C)^2, -(16)^2\delta^8(1-C)^2(B-C)^2C\right).$$

Nous savons par ailleurs que :

* B et $C(1-C)$ sont premiers entre eux ;
* C et $\left((1+C)^2 - 4B\right)$ sont premiers entre eux ;

* les polynômes $1-C$ et $(1+C)^2-4B$ sont premiers entre eux (car $\mathrm{pgcd}(1-C, 1-B) = 1$).

Comme $\mu_{2,3}$ est sans facteur carré, nous déduisons de ces trois relations de primalité relative que $\mu_{2,3}$ divise $\delta(B-C)$. $\square$

Nous donnons maintenant trois applications de la proposition 4.1.7.

Proposition 4.5.5 *Soit k un corps de caractéristique 0. Soient B, C, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-C$, $B-C$ et $(1+C)^2-4B$ soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y + \delta(1+C))(y^2 - 4\delta^2 B)(y^2 - 4\delta^2 C).$$

Nous reprenons les notations 4.5.1 et 4.1. Nous supposons que les hypothèses de la proposition 4.5.2 sont vérifiées. Nous supposons de plus que B et C ne sont pas des carrés dans $k(x)$.
Soit p un facteur premier de $B-C$. Nous supposons que

* *B et C sont premiers entre eux, et*
* *il n'existe pas $\lambda \in k$ tel que $B \equiv \lambda^2 \bmod p$.*

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\alpha_1], [\alpha_2], [\alpha_3])$$

avec α_1, α_2, $\alpha_3 \in k[x]$ trois polynômes tels que

$$v_p(\alpha_2) = 0 \text{ et } v_p(\alpha_3) = 0.$$

Démonstration.

Soit $\mathrm{div}(u,v) \in \mathrm{Div}^0(k(\mathcal{H}))$ un diviseur semi-réduit avec u premier à $L_2 L_3$. Nous notons $\mathrm{Cl}(\mathrm{div}(u,v))$ la classe d'équivalence linéaire de $\mathrm{div}(u,v)$. Nous avons alors

* $\Xi_{\mathcal{H},2}(\mathrm{Cl}(\mathrm{div}(u,v))) = \left[N_{K_2/k(x)}\left((-1)^{\deg(u)}u\right)\right]$ et
* $\Xi_{\mathcal{H},3}(\mathrm{Cl}(\mathrm{div}(u,v))) = \left[N_{K_3/k(x)}\left((-1)^{\deg(u)}u\right)\right]$.

Nous appliquons la proposition 4.1.7 avec $\mathcal{P}$ la place d'uniformisante p et $A := 4\delta^2 B$: comme

* $v_p(B) \equiv 0 \bmod 2$ (car B et $B-C$ sont premiers entre eux), et
* il n'existe pas $\lambda \in k$ tel que $p^{-v_p(B)} B \equiv \lambda^2 \bmod p$,

cette proposition affirme que la valuation $v_p\left(N_{K_2/k(x)}\left((-1)^{\deg(u)}u\right)\right)$ est paire.

La proposition 4.1.7 s'applique aussi avec $\mathcal{P}$ la place d'uniformisante p et $A := 4\delta^2 C$ (car $C \equiv B \bmod p$). Nous en déduisons que la valuation $v_p\left(N_{K_3/k(x)}\left((-1)^{\deg(u)}u\right)\right)$ est paire. $\square$

Proposition 4.5.6 *Soit k un corps de caractéristique 0. Soient B, C, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-C$, $B-C$ et $(1+C)^2-4B$ soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y+\delta(1+C))(y^2-4\delta^2 B)(y^2-4\delta^2 C).$$

Nous reprenons les notations 4.5.1 et 4.1. Nous supposons que les hypothèses de la proposition 4.5.2 sont vérifiées. Nous supposons de plus que B et C ne sont pas des carrés dans $k(x)$.
Soit p un facteur premier de δ. Nous supposons que

* *$v_p(B) \equiv 0 \bmod 2$, et*
* *il n'existe pas $\lambda \in k$ tel que $p^{-v_p(B)}B \equiv \lambda^2 \bmod p$.*

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\alpha_1], [\alpha_2], [\alpha_3])$$

avec α_1, α_2, $\alpha_3 \in k[x]$ trois polynômes tels que $v_p(\alpha_2) = 0$.

Démonstration.

Soit $\mathrm{div}(u,v) \in \mathrm{Div}^0(k(\mathcal{H}))$ un diviseur semi-réduit avec u premier à L_2. Nous notons $\mathrm{Cl}(\mathrm{div}(u,v))$ la classe d'équivalence linéaire de $\mathrm{div}(u,v)$. Nous avons alors $\Xi_{\mathcal{H},2}(\mathrm{Cl}(\mathrm{div}(u,v))) = \left[N_{K_2/k(x)}\left((-1)^{\deg(u)}u\right)\right]$.

Nous appliquons la proposition 4.1.7 avec $\mathcal{P}$ la place d'uniformisante p et $A := 4\delta^2 B$: comme

* $v_p(B) \equiv 0 \bmod 2$, et
* il n'existe pas $\lambda \in k$ tel que $p^{-v_p(B)}B \equiv \lambda^2 \bmod p$,

cette proposition affirme que la valuation $v_p\left(N_{K_2/k(x)}\left((-1)^{\deg(u)}u\right)\right)$ est paire. □

Proposition 4.5.7 *Soit k un corps de caractéristique 0. Soient B, C, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-C$, $B-C$ et $(1+C)^2-4B$ soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y+\delta(1+C))(y^2-4\delta^2 B)(y^2-4\delta^2 C).$$

Nous reprenons les notations 4.5.1 et 4.1. Nous supposons que les hypothèses de la proposition 4.5.2 sont vérifiées. Nous supposons de plus que B et C ne sont pas des carrés dans $k(x)$.
Soit p un facteur premier de δ. Nous supposons que

* *$v_p(C) \equiv 0 \bmod 2$, et*
* *il n'existe pas $\lambda \in k$ tel que $p^{-v_p(C)}C \equiv \lambda^2 \bmod p$.*

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\alpha_1], [\alpha_2], [\alpha_3])$$

avec α_1, α_2, $\alpha_3 \in k[x]$ trois polynômes tels que $v_p(\alpha_3) = 0$.

Démonstration.

Soit $\mathrm{div}(u, v) \in \mathrm{Div}^0(k(\mathcal{H}))$ un diviseur semi-réduit avec u premier à L_3. Nous notons $\mathrm{Cl}(\mathrm{div}(u, v))$ la classe d'équivalence linéaire de $\mathrm{div}(u, v)$. Nous avons alors $\Xi_{\mathcal{H},3}(\mathrm{Cl}(\mathrm{div}(u, v))) = \left[N_{K_3/k(x)}\left((-1)^{\deg(u)}u\right)\right]$.

Nous appliquons la proposition 4.1.7 avec $\mathcal{P}$ la place d'uniformisante p et $A := 4\delta^2 C$: comme

* $v_p(C) \equiv 0 \bmod 2$, et
* il n'existe pas $\lambda \in k$ tel que $p^{-v_p(C)}C \equiv \lambda^2 \bmod p$,

cette proposition affirme que la valuation $v_p\left(N_{K_3/k(x)}\left((-1)^{\deg(u)}u\right)\right)$ est paire. □

Les trois propositions suivantes sont des applications de la proposition 4.1.6.

Proposition 4.5.8 *Soit k un corps de caractéristique 0. Soient B, C, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1 - C$, $B - C$ et $(1 + C)^2 - 4B$ soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y + \delta(1 + C))(y^2 - 4\delta^2 B)(y^2 - 4\delta^2 C).$$

Nous reprenons les notations 4.5.1 et 4.1. Nous supposons que les hypothèses de la proposition 4.5.2 sont vérifiées. Nous supposons de plus que

* *B n'est pas un carré dans $k(x)$, et*
* *C est de degré impair.*

Soit λ le coefficient dominant de C.

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\epsilon_1\alpha_1], [\epsilon_2\alpha_2], [\epsilon_3\alpha_3])$$

avec α_1, α_2, $\alpha_3 \in k[x]$ trois polynômes unitaires et ϵ_1, ϵ_2, $\epsilon_3 \in k^\times$ tels que

* *$\epsilon_3 \sim 1$ si α_3 est de degré pair ;*
* *$\epsilon_3 \sim -\lambda$ si α_3 est de degré impair.*

Démonstration.

Soit $\mathrm{div}(u, v) \in \mathrm{Div}^0(k(\mathcal{H}))$ un diviseur semi-réduit avec u premier à L_3. Nous notons $\mathrm{Cl}(\mathrm{div}(u, v))$ la classe d'équivalence linéaire de $\mathrm{div}(u, v)$. Nous avons alors $\Xi_{\mathcal{H},3}(\mathrm{Cl}(\mathrm{div}(u, v))) = \left[N_{K_3/k(x)}\left((-1)^{\deg(u)}u\right)\right]$. Il existe un polynôme unitaire $\alpha_3 \in k[x]$ et $\epsilon_3 \in k^\times$ tels que $N_{K_3/k(x)}\left((-1)^{\deg(u)}u\right) = \epsilon_3\alpha_3$.

Nous appliquons la proposition 4.1.6 en prenant pour $\mathcal{P}$ la place à l'infini de $k(x)$ et $A := 4\delta^2 C$: comme $A \sim C$, nous avons

* $\epsilon_3 \sim 1$ si α_3 est de degré pair ;
* $\epsilon_3 \sim -\lambda$ si α_3 est de degré impair. $\square$

Proposition 4.5.9 *Soit k un corps de caractéristique 0. Soient B, C, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-C$, $B-C$ et $(1+C)^2-4B$ soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y+\delta(1+C))(y^2-4\delta^2 B)(y^2-4\delta^2 C).$$

Nous reprenons les notations 4.5.1 et 4.1. Nous supposons que les hypothèses de la proposition 4.5.4 sont vérifiées.
Soit p un facteur premier de C. Nous supposons que

* *la valuation $v_p(C)$ est impaire, et*
* *$v_p(\delta) = v_p(B-C) = v_p(1-C) = 0$.*

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\alpha_1], [\alpha_2], [\alpha_3])$$

avec α_1, α_2, $\alpha_3 \in k[x]$ trois polynômes tels que

$$v_p(\alpha_3) = 0 \text{ et } \alpha_3 \sim 1 \bmod p.$$

Démonstration.

Soit $\mathrm{div}(u,v) \in \mathrm{Div}^0(k(\mathcal{H}))$ un diviseur semi-réduit avec u premier à L_3. Nous notons $\mathrm{Cl}(\mathrm{div}(u,v))$ la classe d'équivalence linéaire de $\mathrm{div}(u,v)$. Nous avons alors $\Xi_{\mathcal{H},3}(\mathrm{Cl}(\mathrm{div}(u,v))) = \left[N_{K_3/k(x)}\left((-1)^{\deg(u)}u\right)\right]$. Nous posons

$$\alpha_3 := p^{-v_p(N_{K_3/k(x)}((-1)^{\deg(u)}u))} N_{K_3/k(x)}\left((-1)^{\deg(u)}u\right).$$

Nous avons supposé que $v_p(\delta) = v_p(B-C) = v_p(1-C) = 0$. Ainsi, d'après la proposition 4.5.4, la valuation $v_p\left(N_{K_3/k(x)}\left((-1)^{\deg(u)}u\right)\right)$ est paire. Nous en déduisons que $N_{K_3/k(x)}\left((-1)^{\deg(u)}u\right) \sim \alpha_3$, c'est-à-dire que

$$[\alpha_3] = \left[N_{K_3/k(x)}\left((-1)^{\deg(u)}u\right)\right] = \Xi_{\mathcal{H},3}(\mathrm{Cl}(\mathrm{div}(u,v))).$$

Nous appliquons la proposition 4.1.6 en prenant pour $\mathcal{P}$ la place associée à p et $A := 4\delta^2 C$: nous avons $\alpha_3 \sim 1 \bmod p$. $\square$

Proposition 4.5.10 *Soit k un corps de caractéristique 0. Soient B, C, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1-C$, $B-C$ et $(1+C)^2-4B$ soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y+\delta(1+C))(y^2-4\delta^2 B)(y^2-4\delta^2 C).$$

Nous reprenons les notations 4.5.1 et 4.1. Nous supposons que les hypothèses de la proposition 4.5.4 sont vérifiées.
Soit p un facteur premier de B. Nous supposons que

* *la valuation $v_p(B)$ est impaire et*
* $v_p(\delta) = v_p(B - C) = v_p((1 + C)^2 - 4B) = 0$.

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\alpha_1], [\alpha_2], [\alpha_3])$$

avec α_1, α_2, $\alpha_3 \in k[x]$ trois polynômes tels que

$$v_p(\alpha_2) = 0 \text{ et } \alpha_2 \sim 1 \bmod p.$$

Démonstration.

Soit $\mathrm{div}(u, v) \in \mathrm{Div}^0(k(\mathcal{H}))$ un diviseur semi-réduit avec u premier à L_2. Nous notons $\mathrm{Cl}(\mathrm{div}(u, v))$ la classe d'équivalence linéaire de $\mathrm{div}(u, v)$. Nous avons alors $\Xi_{\mathcal{H},2}(\mathrm{Cl}(\mathrm{div}(u, v))) = \left[N_{K_2/k(x)}\left((-1)^{\deg(u)}u\right)\right]$. Nous posons

$$\alpha_2 := p^{-v_p(N_{K_2/k(x)}((-1)^{\deg(u)}u))} N_{K_2/k(x)}\left((-1)^{\deg(u)}u\right).$$

Nous avons supposé que $v_p(\delta) = v_p(B - C) = v_p((1 + C)^2 - 4B) = 0$. Ainsi, d'après la proposition 4.5.4, la valuation $v_p\left(N_{K_2/k(x)}\left((-1)^{\deg(u)}u\right)\right)$ est paire. Nous en déduisons que $N_{K_2/k(x)}\left((-1)^{\deg(u)}u\right) \sim \alpha_2$, c'est-à-dire que

$$[\alpha_2] = \left[N_{K_2/k(x)}\left((-1)^{\deg(u)}u\right)\right] = \Xi_{\mathcal{H},2}(\mathrm{Cl}(\mathrm{div}(u, v))).$$

Nous appliquons la proposition 4.1.6 en prenant pour $\mathcal{P}$ la place associée à p et $A := 4\delta^2 B$: nous avons $\alpha_2 \sim 1 \bmod p$. □

Proposition 4.5.11 *Soit k un corps de caractéristique 0. Soient B, C, $\delta \in k[x]$ trois polynômes non nuls tels que les polynômes $1 - C$, $B - C$ et $(1 + C)^2 - 4B$ soient non nuls.*

Soit $\mathcal{H}$ la courbe hyperelliptique sur $k(x)$ d'équation affine

$$\mathcal{H} : z^2 = (y + \delta(1 + C))(y^2 - 4\delta^2 B)(y^2 - 4\delta^2 C).$$

Nous reprenons les notations 4.5.1 et 4.1. Nous supposons que les hypothèses de la proposition 4.5.4 sont vérifiées.
Soit p un facteur premier de $B - C$. Nous supposons que

* $v_p(\delta) = v_p(1 - C) = v_p(C) = 0$, *et*
* *il n'existe pas $\lambda \in k$ tel que $C \equiv \lambda^2 \bmod p$.*

Alors tout élément α de l'image de $\Xi_{\mathcal{H}}$ est de la forme

$$\alpha = ([\alpha_1], [\alpha_2], [\alpha_3])$$

avec α_1, α_2, $\alpha_3 \in k[x]$ trois polynômes tels que

$$v_p(\alpha_1) = 0 \text{ et } \alpha_1 \sim 1 \bmod p.$$

Démonstration.

Soit $< u, v > \in \mathrm{Jac}(\mathcal{H})(k(x))$ un $k(x)$-point de $\mathrm{Jac}(\mathcal{H})$. Quitte à ajouter un point de 2-torsion au point $< u, v >$, nous pouvons supposer, sans perte de généralité, que u est premier à $L_1 L_2 L_3$.

Il existe quatre polynômes $\widetilde{u}_0$, $\widetilde{u}_1$, $\widetilde{u}_2$ et λ premiers dans leur ensemble tels que

$$u(y) = \frac{\widetilde{u}_2}{\lambda} y^2 + \frac{\widetilde{u}_1}{\lambda} y + \frac{\widetilde{u}_0}{\lambda}.$$

Puisque u est unitaire, λ est le coefficient dominant du polynôme $\widetilde{u}_2 y^2 + \widetilde{u}_1 y + \widetilde{u}_0$. Ainsi λ est égal à $\widetilde{u}_2$, $\widetilde{u}_1$ ou $\widetilde{u}_0$. Par conséquent, les polynômes $\widetilde{u}_2$, $\widetilde{u}_1$ et $\widetilde{u}_0$ sont premiers entre eux dans leur ensemble.

L'image du point $< u, v >$ par $\Xi_{\mathcal{H}}$ est

$$\Xi_{\mathcal{H}}(< u, v >) = \left(\left[N_{K_i/k(x)} \left((-1)^{\deg(u)} u\left(y_i\right) \right) \right] \right)_{i=1}^{3}$$

Si le polynôme $\lambda^2 N_{K_{3,\mathcal{H}}/k(x)}\left((-1)^{\deg(u)} u\right)$ n'est pas divisible par p :
Comme p divise $B - C$, nous avons

$$\begin{aligned} \lambda^2 N_{K_{3,\mathcal{H}}/k(x)}\left((-1)^{\deg(u)} u\right) &= (\widetilde{u}_0 + 4\delta^2 C \widetilde{u}_2)^2 - 4\delta^2 C \widetilde{u}_1^2 \\ &\equiv (\widetilde{u}_0 + 4\delta^2 B \widetilde{u}_2)^2 - 4\delta^2 B \widetilde{u}_1^2 \bmod p \\ &\equiv \lambda^2 N_{K_{2,\mathcal{H}}/k(x)}\left((-1)^{\deg(u)} u\right) \bmod p. \end{aligned}$$

Le polynôme $\lambda^2 N_{K_{3,\mathcal{H}}/k(x)}\left((-1)^{\deg(u)} u\right)$ est inversible modulo p. Nous en déduisons que

$$\lambda^4 N_{K_{2,\mathcal{H}}/k(x)}\left((-1)^{\deg(u)} u\right) N_{K_{3,\mathcal{H}}/k(x)}\left((-1)^{\deg(u)} u\right) \sim 1 \bmod p.$$

Pour conclure, il suffit d'utiliser la proposition 1.5.9

$$\begin{aligned} \Xi_{\mathcal{H},1}(< u, v >) &= \Xi_{\mathcal{H},2}(< u, v >).\Xi_{\mathcal{H},3}(< u, v >) \\ &= \left[\lambda^4 N_{K_{2,\mathcal{H}}/k(x)}\left((-1)^{\deg(u)} u\right) N_{K_{3,\mathcal{H}}/k(x)}\left((-1)^{\deg(u)} u\right) \right] \\ &= [1]. \end{aligned}$$

Si $\lambda^2 N_{K_{3,\mathcal{H}}/k(x)}\left((-1)^{\deg(u)} u\right)$ est divisible par p, mais pas $\widetilde{u}_1$: nous avons alors

$$\lambda^2 N_{K_{3,\mathcal{H}}/k(x)}\left((-1)^{\deg(u)} u\right) = (\widetilde{u}_0 + 4\delta^2 C \widetilde{u}_2)^2 - 4\delta^2 C \widetilde{u}_1^2,$$

donc $4\delta^2 C \widetilde{u}_1^2 \equiv (\widetilde{u}_0 + 4\delta^2 C \widetilde{u}_2)^2 \bmod p$. Comme $v_p(C) = v_p(\delta) = v_p(\widetilde{u}_1) = 0$, nous en déduisons que $C \sim 1 \bmod p$. Nous avons ainsi une contradiction avec le choix de p. Le cas où $\lambda^2 N_{K_{3,+}/k(x)}\left((-1)^{\deg(u)} u\right)$ est divisible par p et $\widetilde{u}_1$ premier à p est donc impossible.

Si $\widetilde{u}_1$ et $\lambda^2 N_{K_{3,+}/k(x)}\left((-1)^{\deg(u)}u\right)$ sont divisibles par p : la congruence $\lambda^2 N_{K_{3,+}/k(x)}\left((-1)^{\deg(u)}u\right) \equiv 0 \bmod p$ signifie que

$$4\delta^2 C\widetilde{u}_1^2 \equiv (\widetilde{u}_0 + 4\delta^2 C\widetilde{u}_2)^2 \bmod p.$$

Nous savons aussi que p divise $\widetilde{u}_1$. Nous en déduisons donc que :

$$\widetilde{u}_0 \equiv -4\delta^2 C\widetilde{u}_2 \bmod p \tag{4.32}$$

Les polynômes $\widetilde{u}_0$, $\widetilde{u}_1$, et $\widetilde{u}_2$ sont premiers dans leur ensemble. Le polynôme p ne peut donc les diviser tous. Or p divise $\widetilde{u}_1$, donc p ne divise pas l'un des polynômes $\widetilde{u}_0$ et $\widetilde{u}_2$. Ainsi, d'après la congruence 4.32, le polynôme p ne divise pas $\widetilde{u}_2$.

Nous en déduisons la valeur de λ : l'élément λ est le coefficient dominant de $\lambda u = \widetilde{u}_2 y^2 + \widetilde{u}_1 y + \widetilde{u}_0$, c'est-à-dire $\widetilde{u}_2$ (il est non nul puisque premier à p).

En utilisant la relation de congruence 4.32 nous pouvons remarquer que :

$$\begin{aligned}
(-1)^{\deg(u)}\lambda^2 u(\delta(1+C)) &= (-1)^{\deg(u)}\lambda\left(\widetilde{u}_2\delta^2(1+C)^2 - \widetilde{u}_1\delta(1+C) + \widetilde{u}_0\right) \\
&\equiv (-1)^{\deg(u)}\lambda\left(\widetilde{u}_2\delta^2(1+C)^2 - 0 - 4\delta^2 C\widetilde{u}_2\right) \bmod p \\
&\equiv (-1)^{\deg(u)}\lambda\widetilde{u}_2\delta^2(1-C)^2 \bmod p \\
&\equiv (-1)^{\deg(u)}\widetilde{u}_2^2\delta^2(1-C)^2 \bmod p.
\end{aligned}$$

Nous en déduisons

$$(-1)^{\deg(u)}\lambda^2 u(\delta(1+C)) \sim 1 \bmod p$$

car $\widetilde{u}_2\delta(1-C)$ est inversible modulo p et car u est de degré 2. Pour conclure, nous remarquons que

$$\Xi_{\mathcal{H},1}(< u, v >) = \left[(-1)^{\deg(u)}\lambda^2 u(\delta(1+C))\right]. \quad \square$$

Proposition 4.5.12 *Soient η, ω, $\rho \in \mathbb{R}$ des réels. Soit $k := \mathbb{Q}(\eta, \omega, \rho)$. Nous posons :*

$$b_1 = \frac{\rho^2 - \eta^2}{\omega^2 - \eta^2} + \frac{\eta^2 - \omega^2}{4}.$$

Soient $B(x) := (x + b_1)^2 - \eta^2$ et $C(x) := 2(x + b_1) + \omega^2 - \eta^2 - 1$. Nous supposons que les éléments

* η,
* $\left(\omega^2 - \eta^2 - 1\right)^2 - 4\eta^2$ *et* $\left(\omega^2 - \eta^2 - 1\right)^2 - 4\eta^2 - 1$,
* $\left(\omega^2 - \eta^2 - 2\right)^2 - 4\eta^2$ *et* $\left(\omega^2 - \eta^2 - 2\right)^2 - 4\eta^2 - 4$,
* $\left(\omega^2 - \eta^2\right)^2 - 4\eta^2$ *et*
* $B(0) - C(0) = (b_1 - 1)^2 - \omega^2$

sont non nuls.

À tout $\delta \in k(x)^\times$, *nous associons la* $k(x)$*-courbe hyperelliptique* $\widehat{\mathcal{C}}_\delta^+$ *d'équation affine :*

$$\widehat{\mathcal{C}}_\delta^+ : z^2 = (y + \delta(1 + C))(y^2 - 4\delta^2 B)(y^2 - 4\delta^2 C).$$

Nous conservons les notations 4.2 et 4.1. Nous supposons que

* $(1 + \omega)^2 - \eta^2$ *et* $(1 - \omega)^2 - \eta^2$
* $B(0) = b_1^2 - \eta^2$ *et* $C(0) = 2b_1 + \omega^2 - \eta^2 - 1$,

ne sont pas des carrés dans k*. Nous supposons de plus que l'un des deux éléments*

$$\eta^2 - \omega^2 - 2\omega \text{ et } \eta^2 - \omega^2 + 2\omega$$

n'est pas un carré dans k*.*

Alors pour tout $\zeta \in k$ *strictement positif,*

* *l'image de* $\Pi_{\widehat{\mathcal{C}}_\zeta^+}$ *est égale à l'image de la torsion de* $Jac(\widehat{\mathcal{C}}_\zeta^+)(k(x))$ *par* $\Pi_{\widehat{\mathcal{C}}_\zeta^+}$, *et*
* *l'image de* $\Pi_{\widehat{\mathcal{C}}_{\zeta x}^+}$ *est égale à l'image de la torsion de* $Jac(\widehat{\mathcal{C}}_{\zeta x}^+)(k(x))$ *par* $\Pi_{\widehat{\mathcal{C}}_{\zeta x}^+}$.

Démonstration.

Soit $\zeta \in k$ strictement positif et $\delta \in \{\zeta, \zeta x\}$. Soit $\beta \in \mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)(k(x))$.

Le polynôme C est de degré 1. Le polynôme C n'est donc pas un carré dans $k(x)$.

Nous avons supposé le discriminant $4\eta^2$ de B non nul. Ainsi le polynôme $B = (x + b_1)^2 - \eta^2$ n'a pas de racine double. Le polynôme B n'est donc pas un carré.

Le reste de la division euclidienne de $B = (x + b_1)^2 - \eta^2$ par $C = 2(x + b_1) + \omega^2 - \eta^2 - 1$ est

$$\frac{(\omega^2 - \eta^2 - 1)^2}{4} - \eta^2$$

Ce reste est différent de 0 et $\frac{1}{4}$, donc

* B et C sont premiers entre eux, et
* $1 - 4B$ et C sont premiers entre eux.

D'après la seconde relation de primalité, les polynômes $(1 + C)^2 - 4B$ et C sont aussi premiers entre eux.

Le reste $\frac{(\omega^2 - \eta^2 - 2)^2}{4} - \eta^2$ de la division euclidienne de B par $C - 1$ est différent de 0 et 1, donc

* B est premier à $C - 1$ et
* $B - 1$ est premier à $C - 1$.

Finalement, les hypothèses des propositions 4.5.2 et 4.5.4 sont vérifiées. Ainsi, la proposition 4.5.4 s'applique et affirme l'existence

* d'un diviseur sans facteur carré $\mu_{1,2} \in k[x]$ de $\delta((1+C)^2 - 4B)$,
* d'un diviseur sans facteur carré $\mu_{1,3} \in k[x]$ de $\delta(1-C)$ et
* d'un diviseur sans facteur carré $\mu_{2,3} \in k[x]$ de $\delta(B-C)$

tels que $\Xi_{\widehat{\mathcal{C}}_\delta^+}(\beta) = ([\mu_{1,2}\mu_{1,3}], [\mu_{1,2}\mu_{2,3}], [\mu_{1,3}\mu_{2,3}])$.

Le triplet $([(1+C)^2 - 4B], [(1+C)^2 - 4B], [1])$ est l'image par $\Xi_{\widehat{\mathcal{C}}_\delta^+}$ d'un élément de 2-torsion de $\mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)(k(x))$ (voir la proposition 4.5.3). De plus, le polynôme $(1+C)^2 - 4B$ est de degré au plus 1. Ainsi, quitte à ajouter à β un élément de 2-torsion de $\mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)(k(x))$, nous pouvons supposer que $\mu_{1,2}$ est un diviseur de δ.

Soit $p := x + b_1 - 1 - \omega$. Le polynôme p est un des deux facteurs premiers de $B - C = (x + b_1 - 1)^2 - \omega^2$. Le reste de la division euclidienne de $B = (x + b_1)^2 - \eta^2$ par p est

$$(1+\omega)^2 - \eta^2.$$

Par hypothèse, ce reste n'est pas un carré dans k. La proposition 4.5.5 affirme donc que la valuation $v_p(\mu_{1,2}\mu_{2,3})$ est paire. Or $v_p(\mu_{1,2}) = 0$ donc la valuation $v_p(\mu_{2,3})$ est paire. Par symétrie des roles de ω et $-\omega$, la valuation de $\mu_{2,3}$ en $x + b_1 - 1 + \omega$ est paire. Finalement, le polynôme sans facteur carré $\mu_{2,3}$ est un diviseur de δ.

Nous supposons momentanément que $\delta = \zeta x$. Nous avons supposé que $B(0) = b_1^2 - \eta^2$ n'est pas un carré dans k. En particulier, B(0) est non nul. Nous en déduisons que B et x sont premiers entre eux. D'après la proposition 4.5.6 appliqué au cas $p = x$, la valuation $v_x(\mu_{1,2}\mu_{2,3})$ est paire. De même, la proposition 4.5.7 s'applique (car $C(0) = 2b_1 + \omega^2 - \eta^2 - 1$ n'est pas un carré dans $k(x)$) : $v_x(\mu_{1,3}\mu_{2,3})$ est paire.

De plus, les polynômes $\mu_{1,2}$, $\mu_{1,3}$ et $\mu_{2,3}$ sont sans facteur carré. Les valuations $v_x(\mu_{1,2})$, $v_x(\mu_{1,3})$ et $v_x(\mu_{1,2})$ sont donc égales (elles sont égales à 0 ou 1 et de même parité). Or

$$\begin{aligned}\Xi_{\widehat{\mathcal{C}}_\delta^+}(\beta) &= ([\mu_{1,2}\mu_{1,3}], [\mu_{1,2}\mu_{2,3}], [\mu_{1,3}\mu_{2,3}]) \\ &= ([(\delta\mu_{1,2})(\delta\mu_{1,3})], [(\delta\mu_{1,2})(\delta\mu_{2,3})], [(\delta\mu_{1,3})(\delta\mu_{2,3})]),\end{aligned}$$

donc, quitte à les multiplier tous les trois par δ^{-1}, nous pouvons supposer que les polynômes $\mu_{1,2}$, $\mu_{1,3}$ et $\mu_{2,3}$ sont premiers à δ.

Nous revenons au cas général ($\delta \in \{\zeta, \zeta x\}$). Nous nous sommes ramenés au cas où

* $\mu_{1,2} \in k^\times$ est une constante,

* $\mu_{1,3} \in k[x]$ est un diviseur sans facteur carré de $(1-C)$, et
* $\mu_{2,3} \in k^\times$ est une constante.

Comme $C-1$ est de degré 1, le polynôme $\mu_{1,3}$ ne peut prendre que deux valeurs différentes à une constante près : il existe $\epsilon \in k^\times$ tel que $\mu_{1,3} = \epsilon$ ou $\mu_{1,3} = \epsilon(1-C)$. En fait, d'après la proposition 4.5.8, et puisque $1-C$ et $-C$ ont même coefficient dominant, nous avons $\mu_{2,3}\epsilon \sim 1$.

Comme $\eta \neq 0$, le polynôme B est sans facteur carré. Par ailleurs,

* $\operatorname{pgcd}(B, C) = 1$ donc B et $B-C$ sont premiers entre eux ;
* $B(0) = b_1^2 - \eta^2 \neq 0$ donc B est premier à δ ;
* le reste $\frac{1}{4}\left(\left(\omega^2-\eta^2\right)^2 - 4\eta^2\right)$ de la division euclidienne du polynôme $B = (x+b_1) - \eta^2$ par $1 + C = 2\,(x+b_1) + \omega^2 - \eta^2$ est non nul, donc $\operatorname{pgcd}(1+C, B) = 1$ et donc les polynômes $(1+C)^2 - 4B$ et B sont premiers entre eux.

La proposition 4.5.10 s'applique donc : nous avons $\mu_{1,2}\mu_{2,3} \sim 1 \bmod p$ pour tout facteur premier p de B. Le polynôme $\mu_{1,2}\mu_{2,3}$ étant une constante, nous en déduisons que $\mu_{1,2} \sim \mu_{2,3} \sim \epsilon$. En particulier, nous avons

$$\mu_{1,2}\mu_{1,3} \sim 1 \text{ ou } \mu_{1,2}\mu_{1,3} \sim 1 - C.$$

Nous supposons que $\mu_{1,2}\mu_{1,3} \sim 1 - C$. Comme B est premier à C, les polynômes $B-C$ et C sont premiers entre eux. De même, puisque $\operatorname{pgcd}(B-1, C-1) = 1$, le polynôme $B-C$ est premier à $C-1$. De plus, $B(0) \neq C(0)$ donc les polynômes $B-C$ et δ sont premiers entre eux. Par ailleurs,

* le polynôme $B-C$ se factorise sous la forme

$$B - C = (x + b_1 - 1 + \omega)(x + b_1 - 1 - \omega),$$

* le reste $(\omega+1)^2 - \eta^2$ de la division euclidienne de

$$C = 2(x + b_1 - 1) + \omega^2 - \eta^2 - 1$$

par $x + b_1 - 1 - \omega$ n'est pas un carré dans k, et

* le reste $(\omega+1)^2 - \eta^2$ de la division euclidienne de

$$C = 2(x + b_1 - 1) + \omega^2 - \eta^2 - 1$$

par $x + b_1 - 1 + \omega$ n'est pas un carré dans k.

Les hypothèses de la proposition 4.5.11 sont donc satisfaites pour tous les facteurs premiers de $B-C$.

Cette proposition affirme que $\mu_{1,2}\mu_{1,3} \sim 1 \bmod p$ pour tout facteur premier p de $B-C = (x+b_1-1)^2 - \omega^2$. Puisque $1-C = -2(x+b_1-1) + \eta^2 - \omega^2$, cela signifie que les deux éléments

$$\eta^2 - \omega^2 - 2\omega \text{ et } \eta^2 - \omega^2 + 2\omega$$

sont des carrés dans k. Ce n'est pas le cas, donc $\mu_{1,2}\mu_{1,3} \sim 1$. Par suite, l'image

$$\Xi_{\widehat{\mathcal{C}}_\delta^+}(\beta) = \left([\mu_{1,2}\mu_{1,3}], [\mu_{1,2}\mu_{2,3}], [\mu_{1,3}\mu_{2,3}]\right)$$

est triviale.

Nous venons ainsi de montrer que, pour tout $\beta \in \mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)(k(x))$, il existe un point de torsion $T \in \mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)(k(x))$ tel que l'image $\Xi_{\widehat{\mathcal{C}}_\delta^+}(\beta + T)$ soit triviale. Pour conclure il suffit de remarquer que $\Pi_{\widehat{\mathcal{C}}_\delta^+} = \Xi_{\widehat{\mathcal{C}}_\delta^+}$. $\square$

4.6 Conclusion : une famille de polynômes qui ne sont pas somme de trois carrés dans $\mathbb{R}(x, y)$.

Théorème 4.6.1 *Soient η, ω, $\rho \in \mathbb{R}$ des réels. Soit $k := \mathbb{Q}(\eta, \omega, \rho)$. Nous posons :*

$$b_1 = \frac{\rho^2 - \eta^2}{\omega^2 - \eta^2} + \frac{\eta^2 - \omega^2}{4}.$$

Soient $B(x) := (x + b_1)^2 - \eta^2$ et $C(x) := 2(x + b_1) + \omega^2 - \eta^2 - 1$. Nous supposons que les éléments

- *η et ρ,*
- *$\omega^2 - \eta^2 - 2 - 2\eta$ et $\omega^2 - \eta^2 - 2 + 2\eta$,*
- *$\left(\omega^2 - \eta^2 - 2\right)^2 - 4\eta^2 - 4$,*
- *$\omega^2 - \eta^2 - 1 + 2\eta$ et $\omega^2 - \eta^2 - 1 - 2\eta$,*
- *$\left(\omega^2 - \eta^2 - 1\right)^2 - 4\eta^2 - 1$,*
- *$\omega^2 - \eta^2 - 2\eta$ et $\omega^2 - \eta^2 + 2\eta$*

sont non nuls.

Nous supposons de plus $\omega > 1 + |\eta|$, $\omega^2 - \eta^2 > 2\omega$, $b_1 > 1 + \frac{\omega^2 - \eta^2}{2}$ et qu'aucun des éléments

a. $\left(\left(\omega^2 - \eta^2\right)^2 - 4\omega^2\right) = \left(\omega^2 - \eta^2 - 2\omega\right)\left(\omega^2 - \eta^2 + 2\omega\right)$

b. $(2b_1 - 2 + \omega^2 - \eta^2)(\omega^2 - \eta^2 - 2\omega)$,

c. $(2b_1 - 2 + \omega^2 - \eta^2)(\omega^2 - \eta^2 + 2\omega)$,

d. $2(\omega^2 - \eta^2 - 2\omega)(b_1 - 1 - \omega)$,

e. $2(\omega^2 - \eta^2 + 2\omega)(b_1 - 1 + \omega)$

f. $2\left(2b_1 - 2 + \omega^2 - \eta^2\right)(b_1 - 1 + \omega)$,

g. $2\left(2b_1 - 2 + \omega^2 - \eta^2\right)(b_1 - 1 - \omega)$,

h. $\left((b_1 - 1)^2 - \omega^2\right)\left(\left(\omega^2 - \eta^2\right)^2 - 4\omega^2\right)$

i. $2\left(\omega^2 - \eta^2\right)\left(\omega^2 - \eta^2 - 2\omega\right)\left((\omega + 1)^2 - \eta^2\right)^n$ *(pour $n \in \{0, 1\}$)*,

j. $2\left(\omega^2 - \eta^2\right)\left(\omega^2 - \eta^2 + 2\omega\right)\left((\omega - 1)^2 - \eta^2\right)^n$ *(pour $n \in \{0, 1\}$)*

k. $\left((b_1-1)^2-\omega^2\right)^{n_1}\left((\omega-1)^2-\eta^2\right)^{n_2}\left((\omega+1)^2-\eta^2\right)^{n_3}$ *(avec* (n_1,n_2,n_3) *un triplet non nul d'éléments de* $\{0,1\}$*),*

l. $2\left(\omega^2-\eta^2\right)\left(2b_1-2+\omega^2-\eta^2\right)$,

m. $2^{n_1}\left(\omega^2-\eta^2+2\omega\right)(b_1-1+\omega)\left(\omega^2-\eta^2\right)^{n_1}\left(2b_1-2+\omega^2-\eta^2\right)^{1-n_1}$ $\times(\omega-1-\eta)^{1-n_2}(\omega-1+\eta)^{n_2}$ *(avec* n_1, $n_2\in\mathbb{N}$*), et*

n. $2^{1-n_1}\left(\omega^2-\eta^2+2\omega\right)\left(\omega^2-\eta^2\right)^{n_1}\left(2b_1-2+\omega^2-\eta^2\right)^{n_1}$ $\times(\omega-1-\eta)^{1-n_2}(\omega-1+\eta)^{n_2}$, *(avec* n_1, $n_2\in\mathbb{N}$*)*

o. $b_1^2-\eta^2$, *et*

p. $2b_1+\omega^2-\eta^2-1$,

n'est un carré dans k.

Alors le polynôme

$$P(x,y):=\left(y^2+1\right)\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right)$$

est positif ou nul sur $\mathbb{R}^2$*, mais n'est pas une somme de trois carrés dans* $\mathbb{R}(x,y)$.

Démonstration.

Des trois inégalités $b_1>1+\frac{\omega^2-\eta^2}{2}$, $\frac{\omega^2-\eta^2}{2}>\omega$ et $\omega>1+|\eta|$, nous déduisons que l'élément b_1 est strictement supérieur à $2+|\eta|$ et donc strictement positif. En particulier, nous avons $b_1>0$ et $b_1^2>\eta^2$. Ainsi, le polynôme

$$B(x^2)=x^4+2b_1x^2+b_1^2-\eta^2$$

est positif ou nul sur $\mathbb{R}$.

De même, puisque $2b_1>2+\omega^2-\eta^2$ et $\omega^2>\eta^2$, les éléments $2b_1-2+\omega^2-\eta^2=\left(2b_1-2-\left(\omega^2-\eta^2\right)\right)+2\left(\omega^2-\eta^2\right)$ et $2b_1-1+\omega^2-\eta^2$ sont strictement positifs. Ainsi, le polynôme

$$C(x^2):=2x^2+\left(2b_1-1+\omega^2-\eta^2\right)$$

est positif ou nul sur $\mathbb{R}$. Par conséquent, le polynôme

$$P(x,y)=\left(y^2+1\right)\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right)$$

est positif ou nul sur $\mathbb{R}^2$.

Le reste $\left(C\left(x^2\right)-1\right)\left(B\left(x^2\right)-C\left(x^2\right)\right)$ de la division euclidienne de

$$\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right)$$

par y^2+1 est non nul (il est même de degré 6 en y). Les polynômes y^2+1 et $\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right)$ sont donc premiers entre eux.

De même, le reste $\left(B\left(x^2\right)-C\left(x^2\right)\right)$ de la division euclidienne de $y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)$ par $y^2+C\left(x^2\right)$ est non nul, donc les polynômes $y^2+C\left(x^2\right)$ et $y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)$ sont premiers entre eux.

Par ailleurs, le polynôme $C\left(x^2\right)$ est non nul, donc le polynôme $y^2+\left(C\left(x^2\right)\right)$ est sans facteur carré.

Enfin, le discriminant $16B\left(x^2\right)\left(\left(1+C\left(x^2\right)\right)^2-4B\left(x^2\right)\right)^2$ du polynôme $y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)$ est non nul donc $y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)$ est sans facteur carré. Ainsi, des relations de primalité précédentes, nous déduisons que le polynôme $P(x,y)\in k[x][y]$ est sans facteur carré. En particulier, les hypothèses de la proposition 1.2.8 sont satisfaites.

Nous montrons maintenant que $P(x,y)$ n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$. Pour cela, nous introduisons la courbe hyperelliptique $\mathcal{C}$ sur $\mathbb{R}(x)$ d'équation affine

$$\mathcal{C}: z^2+\left(y^2+1\right)\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right)=0.$$

D'après la proposition 1.2.8, le polynôme $P(x,y)$ est une somme de trois carrés dans $\mathbb{R}(x,y)$ si et seulement si la jacobienne $\mathrm{Jac}(\mathcal{C})$ a un point $\mathbb{R}(x)$-rationnel antineutre.

Nous commençons par montrer que le groupe $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est de rang de Mordell-Weil nul, c'est-à-dire égal à son sous-groupe de torsion. Pour cela, nous utilisons la proposition 3.5.3.6.

Nous avons supposé $\omega>1+|\eta|$, donc ω est non nul. De même, $\omega^2-\eta^2>2|\omega|$, donc $\omega^2-\eta^2$, $\omega^2-\eta^2+2\omega$ et $\omega^2-\eta^2-2\omega$ sont non nuls (ils sont même strictement positifs).

Par ailleurs les éléments $2b_1+\omega^2-\eta^2-1$, $b_1^2-\eta^2$ et $(b_1-1)^2-\omega^2$ ne sont pas des carrés dans k, donc les éléments $2b_1+\omega^2-\eta^2-1$, $b_1+\eta$, $b_1-\eta$, $b_1-1+\omega$ et $b_1-1-\omega$ sont non nuls. Nous venons ainsi de montrer que les éléments

* η, ω, ρ et $\omega^2-\eta^2$,
* $2b_1-2+\omega^2-\eta^2$,
* $\omega^2-\eta^2-2-2\eta$ et $\omega^2-\eta^2-2+2\eta$,
* $\omega^2-\eta^2+2\omega$ et $\omega^2-\eta^2-2\omega$,
* $\omega^2-\eta^2-1+2\eta$ et $\omega^2-\eta^2-1-2\eta$,
* $2b_1+\omega^2-\eta^2-1$, $b_1+\eta$, $b_1-\eta$, $b_1-1+\omega$ et $b_1-1-\omega$

sont non nuls. Les hypothèses de la proposition 3.5.3.6 sont donc vérifiées.

Afin d'utiliser la proposition 3.5.3.6, nous associons à tout $\delta \in k(x)^\times$ les deux $k(x)$-courbes hyperelliptiques $\mathcal{C}_\delta^+$ et $\widehat{\mathcal{C}}_\delta^+$ (qui sont de genre 2), et les deux $k(x)$-courbes elliptiques $\mathcal{C}_\delta^-$ et $\widehat{\mathcal{C}}_\delta^-$ d'équations affines respectives :

$$\mathcal{C}_\delta^+ : z^2 = \left(y + \tfrac{\delta(1+C(x))}{2}\right)\left(y^2 - \left(\tfrac{\delta(1-C(x))}{2}\right)^2\right)\left(y^2 - \tfrac{\delta^2[(1+C(x))^2-4B(x)]}{4}\right)$$

$$\widehat{\mathcal{C}}_\delta^+ : z^2 = \left(y + \delta\left(1 + C\left(x\right)\right)\right)\left(y^2 - 4\delta^2 B\left(x\right)\right)\left(y^2 - 4\delta^2 C\left(x\right)\right)$$

$$\mathcal{C}_\delta^- : z^2 = y\left(y^2 - \delta\left[\left(1 - C\left(x\right)\right)^2 - 2\left(B\left(x\right) - C\left(x\right)\right)\right]y + \delta^2\left(B\left(x\right) - C\left(x\right)\right)^2\right)$$

$$\widehat{\mathcal{C}}_\delta^- : t^2 = y\left(y + \delta\left(1 - C\left(x\right)\right)^2\right)\left(y + \delta\left(\left(1 - C\left(x\right)\right)^2 - 4\left(B\left(x\right) - C\left(x\right)\right)\right)\right).$$

Nous reprenons les notations 4.2 et 4.4.

D'après la proposition 3.5.3.6, le $\mathbb{R}(x)$-rang de Mordell-Weil de la jacobienne de la courbe $\mathcal{C}$ est nul si et seulement si, pour tout $\zeta \in k$ strictement positif, les images des homomorphismes

$$\gamma_{\mathcal{C}_\zeta^-},\ \gamma_{\mathcal{C}_{\zeta x}^-},\ \gamma_{\widehat{\mathcal{C}}_\zeta^-},\ \gamma_{\widehat{\mathcal{C}}_{\zeta x}^-},\ \Pi_{\mathcal{C}_\zeta^+},\ \Pi_{\mathcal{C}_{\zeta x}^+},\ \Pi_{\widehat{\mathcal{C}}_\zeta^+} \text{ et } \Pi_{\widehat{\mathcal{C}}_{\zeta x}^+}$$

sont respectivement les images des points de torsion $k(x)$-rationnels de

$$\mathcal{C}_\zeta^-,\ \mathcal{C}_{\zeta x}^-,\ \widehat{\mathcal{C}}_\zeta^-,\ \widehat{\mathcal{C}}_{\zeta x}^-,\ \mathrm{Jac}(\mathcal{C}_\zeta^+),\ \mathrm{Jac}(\mathcal{C}_{\zeta x}^+),\ \mathrm{Jac}(\widehat{\mathcal{C}}_\zeta^+) \text{ et } \mathrm{Jac}(\widehat{\mathcal{C}}_{\zeta x}^+).$$

Nous étudions maintenant les images des homomorphismes

$$\gamma_{\mathcal{C}_\zeta^-},\ \gamma_{\mathcal{C}_{\zeta x}^-},\ \gamma_{\widehat{\mathcal{C}}_\zeta^-},\ \gamma_{\widehat{\mathcal{C}}_{\zeta x}^-},\ \Pi_{\mathcal{C}_\zeta^+},\ \Pi_{\mathcal{C}_{\zeta x}^+},\ \Pi_{\widehat{\mathcal{C}}_\zeta^+} \text{ et } \Pi_{\widehat{\mathcal{C}}_{\zeta x}^+}$$

en utilisant les propositions 4.2.5, 4.2.7, 4.3.5, 4.3.6, 4.4.4.1, 4.4.4.2 et 4.5.12.

1. Les hypothèses de la proposition 4.2.5 sont vérifiées :
   * $\omega^2 > \eta^2$, et
   * $\left(\left(\omega^2 - \eta^2\right) - 4\omega^2\right) = \left(\omega^2 - 2\omega - \eta^2\right)\left(\omega^2 + 2\omega - \eta^2\right)$ n'est pas un carré dans k.

Par conséquent, pour tout $\zeta \in k$ strictement positif, l'image du morphisme $\gamma_{\mathcal{C}_\zeta^-}$ est triviale.

2. Comme $\omega^2 > \eta^2$ et comme les éléments
   * $(b_1 - 1)^2 - \omega^2$ (voir l'hypothèse $k.$),
   * $(2b_1 - 2 + \omega^2 - \eta^2)(\omega^2 - \eta^2 + 2\omega)$,
   * $(2b_1 - 2 + \omega^2 - \eta^2)(\omega^2 - \eta^2 - 2\omega)$,

* $2(\omega^2-\eta^2-2\omega)(b_1-1-\omega)$, et
* $2(\omega^2-\eta^2+2\omega)(b_1-1+\omega)$

ne sont pas des carrés dans k, les hypothèses de la proposition 4.2.7 sont satisfaites. Nous déduisons de cette proposition que, pour tout $\zeta \in k$ strictement positif, l'image du morphisme $\gamma_{\mathcal{C}^-_{\zeta x}}$ est triviale.

3. Puisque $\omega^2-\eta^2 > 2|\omega|$, l'élément

$$(\omega^2-\eta^2-2\omega)(\omega^2-\eta^2+2\omega)$$

est strictement positif. La proposition 4.3.5 s'applique donc : pour tout $\zeta \in k$ strictement positif, l'image de $\gamma_{\widehat{\mathcal{C}}^-_{\zeta},k(x)}$ est l'image des points de 2-torsion de $\widehat{\mathcal{C}}^-_{\zeta}(k(x))$.

4. Les hypothèses de la proposition 4.3.6 sont vérifiées : les éléments $\omega^2-\eta^2$ et ρ sont non nuls (en fait $\omega^2 > \eta^2$), et les éléments
* $(b_1-1)^2-\omega^2$ (voir l'hypothèse $k.$),
* $\left(\omega^2-\eta^2\right)^2-4\omega^2$,
* $2\left(2b_1-2+\omega^2-\eta^2\right)(b_1-1+\omega)$,
* $2\left(2b_1-2+\omega^2-\eta^2\right)(b_1-1-\omega)$ et
* $\left((b_1-1)^2-\omega^2\right)\left(\left(\omega^2-\eta^2\right)^2-4\omega^2\right)$

ne sont pas des carrés dans k. Ainsi, pour tout $\zeta \in k$ strictement positif, l'image de $\gamma_{\widehat{\mathcal{C}}^-_{\zeta x},k(x)}$ est l'image des points de 2-torsion de $\widehat{\mathcal{C}}^-_{\zeta x}(k(x))$.

5. De l'inégalité $\omega^2-\eta^2 > 2|\omega|$ nous déduisons

$$\left(\omega^2-\eta^2\right)^2-2\omega^2-2\eta^2 > 4\omega^2-2\omega^2-2\eta^2 = 2\left(\omega^2-\eta^2\right) > 0.$$

En particulier, l'élément $\left(\omega^2-\eta^2\right)^2-2\omega^2-2\eta^2$ est non nul. Par ailleurs, nous avons supposé que les éléments
* $\left(\omega^2-\eta^2-1\right)^2-4\eta^2 = \left(\omega^2-\eta^2-1+2\eta\right)\left(\omega^2-\eta^2-1-2\eta\right)$ et
* $\left(\omega^2-\eta^2-2\right)^2-4\eta^2 = \left(\omega^2-\eta^2-2+2\eta\right)\left(\omega^2-\eta^2-2-2\eta\right)$

sont non nuls. De plus, aucun des éléments
* $\left((\omega-1)^2-\eta^2\right)^{n_1}\left((\omega+1)^2-\eta^2\right)^{n_2}$ (avec $(n_1,n_2) \in \{(0,1),(1,0),(1,1)\}$) (voir l'hypothèse $k.$),
* $2\left(\omega^2-\eta^2\right)\left(\omega^2-\eta^2-2\omega\right)\left((\omega+1)^2-\eta^2\right)^n$ (avec $n \in \{0,1\}$) et
* $2\left(\omega^2-\eta^2\right)\left(\omega^2-\eta^2+2\omega\right)\left((\omega-1)^2-\eta^2\right)^n$ (avec $n \in \{0,1\}$)

n'est un carré dans k. Or $\omega > 1+|\eta|$, donc les hypothèses de la proposition 4.4.4.1 sont satisfaites. Par suite, pour tout $\zeta \in k$ strictement positif, l'image de $\Pi_{\mathcal{C}^+_{\zeta}}$ est engendrée par l'image des points de torsion 2-primaire

de $\mathrm{Jac}(\mathcal{C}_\zeta^+)(k(x))$.

6. Les éléments
   * $\left(\omega^2-\eta^2-1\right)^2-4\eta^2=\left(\omega^2-\eta^2-1+2\eta\right)\left(\omega^2-\eta^2-1-2\eta\right)$ et
   * $\left(\omega^2-\eta^2-2\right)^2-4\eta^2=\left(\omega^2-\eta^2-2+2\eta\right)\left(\omega^2-\eta^2-2-2\eta\right)$

sont non nuls.

Nous avons supposé $\omega^2-\eta^2>2\omega$, $b_1>1+\frac{\omega^2-\eta^2}{2}$ et $\omega>|\eta|+1$. Par ailleurs, aucun des éléments

   * $\left((b_1-1)^2-\omega^2\right)^{n_1}\left((\omega-1)^2-\eta^2\right)^{n_2}\left((\omega+1)^2-\eta^2\right)^{n_3}$ (avec (n_1,n_2,n_3) un triplet non nul d'éléments de $\{0,1\}$),
   * $2\left(\omega^2-\eta^2\right)\left(2b_1-2+\omega^2-\eta^2\right)$,
   * $2^{n_1}\left(\omega^2-\eta^2+2\omega\right)(b_1-1+\omega)\left(\omega^2-\eta^2\right)^{n_1}\left(2b_1-2+\omega^2-\eta^2\right)^{1-n_1}$ $\times(\omega-1-\eta)^{1-n_2}(\omega-1+\eta)^{n_2}$ (avec n_1, $n_2\in\mathbb{N}$), et
   * $2^{1-n_1}\left(\omega^2-\eta^2+2\omega\right)\left(\omega^2-\eta^2\right)^{n_1}\left(2b_1-2+\omega^2-\eta^2\right)^{n_1}$ $\times(\omega-1-\eta)^{1-n_2}(\omega-1+\eta)^{n_2}$ (avec n_1, $n_2\in\mathbb{N}$)

n'est un carré dans k. Ainsi, les hypothèses de la proposition 4.4.4.2 sont satisfaites. Nous en déduisons que, pour tout $\zeta\in k^\times$ strictement positif, l'image de $\Pi_{\mathcal{C}_{\zeta x}^+}$ est engendrée par l'image des points de torsion 2-primaire de $\mathrm{Jac}(\mathcal{C}_{\zeta x}^+)(k(x))$.

7. Nous avons supposé que l'élément $\left((b_1-1)^2-\omega^2\right)\left(\left(\omega^2-\eta^2\right)^2-4\omega^2\right)$ n'est pas un carré dans k. Par suite, $(b_1-1)^2-\omega^2$ est non nul. Nous avons aussi supposé que les éléments
   * η,
   * $\left(\omega^2-\eta^2-1\right)^2-4\eta^2$ et $\left(\omega^2-\eta^2-1\right)^2-4\eta^2-1$,
   * $\left(\omega^2-\eta^2-2\right)^2-4\eta^2$ et $\left(\omega^2-\eta^2-2\right)^2-4\eta^2-4$, et
   * $\left(\omega^2-\eta^2\right)^2-4\eta^2=\left(\omega^2-\eta^2+2\eta\right)\left(\omega^2-\eta^2-2\eta\right)$

sont non nuls. Par ailleurs, l'élément

$$\left(\omega^2-\eta^2\right)^2-4\omega^2=\left(\omega^2-\eta^2-2\omega\right)\left(\omega^2-\eta^2+2\omega\right)$$

n'est pas un carré dans k, donc
   * $\eta^2-\omega^2-2\omega$ n'est pas un carré dans k ou
   * $\eta^2-\omega^2+2\omega$ n'est pas un carré dans k

Ainsi, puisque les éléments
   * $(1+\omega)^2-\eta^2$ et $(1-\omega)^2-\eta^2$ (voir l'hypothèse $k.$),
   * $b_1^2-\eta^2$ et
   * $2b_1+\omega^2-\eta^2-1$,

ne sont pas des carrés dans k, la proposition 4.5.12 s'applique : pour tout $\zeta \in k$ strictement positif,

* l'image de $\Pi_{\widehat{\mathcal{C}}^+_\zeta}$ est égale à l'image de la torsion de $\mathrm{Jac}(\widehat{\mathcal{C}}^+_\zeta)(k(x))$ par $\Pi_{\widehat{\mathcal{C}}^+_\zeta}$, et
* l'image de $\Pi_{\widehat{\mathcal{C}}^+_{\zeta x}}$ est égale à l'image de la torsion de $\mathrm{Jac}(\widehat{\mathcal{C}}^+_{\zeta x})(k(x))$ par $\Pi_{\widehat{\mathcal{C}}^+_{\zeta x}}$.

Finalement, pour tout $\zeta \in k$ strictement positif, les images des homomorphismes

$$\gamma_{\mathcal{C}^-_\zeta},\ \gamma_{\mathcal{C}^-_{\zeta x}},\ \gamma_{\widehat{\mathcal{C}}^-_\zeta},\ \gamma_{\widehat{\mathcal{C}}^-_{\zeta x}},\ \Pi_{\mathcal{C}^+_\zeta},\ \Pi_{\mathcal{C}^+_{\zeta x}},\ \Pi_{\widehat{\mathcal{C}}^+_\zeta} \text{ et } \Pi_{\widehat{\mathcal{C}}^+_{\zeta x}}$$

sont respectivement les images des points de torsion $k(x)$-rationnels de

$$\mathcal{C}^-_\zeta,\ \mathcal{C}^-_{\zeta x},\ \widehat{\mathcal{C}}^-_\zeta,\ \widehat{\mathcal{C}}^-_{\zeta x},\ \mathrm{Jac}(\mathcal{C}^+_\zeta),\ \mathrm{Jac}(\mathcal{C}^+_{\zeta x}),\ \mathrm{Jac}(\widehat{\mathcal{C}}^+_\zeta) \text{ et } \mathrm{Jac}(\widehat{\mathcal{C}}^+_{\zeta x}).$$

Nous déduisons alors de la proposition 3.5.3.6 que le groupe $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est de rang de Mordell-Weil nul, c'est-à-dire qu'il est égal à son sous-groupe de torsion.

Comme expliqué lors de la sous-section 3.4.2, sous les hypothèse du théorème 4.6.1, aucun des polynômes

$$\begin{array}{l}(1+C(x^2))^2-4B(x^2),\ B(x^2),\ C(x^2),\ B(x^2)C(x^2),\\ B(x^2)-C(x^2) \text{ et } (B(x^2)-C(x^2))(1-C(x^2))\end{array}$$

n'est un carré dans $\mathbb{C}(x)$. Nous sommes donc sous les hypothèses du théorème 2.4.9. Par suite, la jacobienne $\mathrm{Jac}(\mathcal{C})$ n'a aucun $\mathbb{R}(x)$-point de torsion antineutre, et donc aucun $\mathbb{R}(x)$-point antineutre (le groupe $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ est égal à son sous-groupe de torsion).

De plus, d'après la proposition 1.2.8, le polynôme $P(x,y)$ est une somme de trois carrés dans $\mathbb{R}(x,y)$ si et seulement si la jacobienne $\mathrm{Jac}(\mathcal{C})$ a un point $\mathbb{R}(x)$-rationnel antineutre. Par conséquent, le polynôme $P(x,y)$ n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$. □

Corollaire 4.6.2 *Soient η, ω, $\rho \in \mathbb{R}$ trois nombres réels algébriquement indépendants sur $\mathbb{Q}$. Nous posons :*

$$b_1 = \frac{\rho^2-\eta^2}{\omega^2-\eta^2} + \frac{\eta^2-\omega^2}{4}.$$

Soient $B(x) := (x+b_1)^2-\eta^2$ et $C(x) := 2(x+b_1)+\omega^2-\eta^2-1$. Nous supposons que $\omega > 1+|\eta|$, $\omega^2-\eta^2 > 2\omega$, et $b_1 > 1+\frac{\omega^2-\eta^2}{2}$.

Alors le polynôme

$$P(x,y) := \left(y^2+1\right)\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right)$$

est positif ou nul sur $\mathbb{R}^2$*, mais n'est pas une somme de trois carrés dans* $\mathbb{R}(x,y)$*.*

Démonstration.

Soit $k := \mathbb{Q}(\eta,\omega,\rho)$. Puisque les éléments η, ω et ρ sont algébriquement indépendants, l'anneau $\mathbb{Q}[\eta,\omega,\rho]$ est isomorphe à l'anneau des polynômes en trois variables à coefficients dans $\mathbb{Q}$.

Les éléments η, ω et ρ sont algébriquement indépendants, donc les éléments η, ω et $b_1 = \frac{1}{\omega^2-\eta^2}\rho^2 + \left(\frac{-\eta^2}{\omega^2-\eta^2} + \frac{\eta^2-\omega^2}{4}\right)$ sont algébriquement indépendants. En particulier, les éléments

* η et ρ,
* $\omega^2-\eta^2-2-2\eta$ et $\omega^2-\eta^2-2+2\eta$,
* $\left(\omega^2-\eta^2-2\right)^2-4\eta^2-4$,
* $\omega^2-\eta^2-1+2\eta$ et $\omega^2-\eta^2-1-2\eta$,
* $\left(\omega^2-\eta^2-1\right)^2-4\eta^2-1$,
* $\omega^2-\eta^2-2\eta$ et $\omega^2-\eta^2+2\eta$

sont non nuls.

Le polynôme $2\left(\omega^2-\eta^2+2\omega\right) \in \mathbb{Q}(\omega)[\eta]$ est de degré 2 et son discriminant $16\left(\omega^2+2\omega\right)$ est non nul (ω est transcendant sur $\mathbb{Q}$). Par conséquent, le polynôme $2\left(\omega^2-\eta^2+2\omega\right) \in \mathbb{Q}(\omega)[\eta]$ est non constant et sans facteur carré.

De même, les polynômes $2\left(\omega^2-\eta^2-2\omega\right) \in \mathbb{Q}(\omega)[\eta]$ et $\omega^2-\eta^2 \in \mathbb{Q}(\omega)[\eta]$ sont de degrés 2 et leurs discriminants (respectivement $16(\omega^2-2\omega)$ et $4\omega^2$) sont non nuls. Les polynômes $2\left(\omega^2-\eta^2-2\omega\right) \in \mathbb{Q}(\omega)[\eta]$ et $\omega^2-\eta^2 \in \mathbb{Q}(\omega)[\eta]$ sont donc non constants et sans facteur carré.

Les polynômes $\omega+1+\eta \in \mathbb{Q}(\omega)[\eta]$, $\omega+1-\eta \in \mathbb{Q}(\omega)[\eta]$, $\omega-1+\eta \in \mathbb{Q}(\omega)[\eta]$ et $\omega-1-\eta \in \mathbb{Q}(\omega)[\eta]$ sont irréductibles de degrés 1. Ils sont donc non constants et sans facteur carré.

Les polynômes $2\left(\omega^2-\eta^2+2\omega\right) \in \mathbb{Q}(\omega)[\eta]$, $2\left(\omega^2-\eta^2-2\omega\right) \in \mathbb{Q}(\eta)[\omega]$ et $\omega^2-\eta^2 \in \mathbb{Q}(\eta)[\omega]$ sont deux à deux premiers entre eux (leurs différences deux à deux sont des éléments non nuls de $\mathbb{Q}(\omega)$) .

Par division euclidienne, et en remarquant que ω est transcendant sur $\mathbb{Q}$, nous montrons aussi que les polynômes $\omega+1+\eta \in \mathbb{Q}(\omega)[\eta]$, $\omega+1-\eta \in \mathbb{Q}(\omega)[\eta]$, $\omega-1+\eta \in \mathbb{Q}(\omega)[\eta]$ et $\omega-1-\eta \in \mathbb{Q}(\omega)[\eta]$ sont deux à deux premiers entre eux et premiers aux polynômes $2\left(\omega^2-\eta^2+2\omega\right)$, $2\left(\omega^2-\eta^2-2\omega\right)$ et $\omega^2-\eta^2$.

Finalement, les polynômes

* $2\left(\omega^2-\eta^2+2\omega\right)\in\mathbb{Q}(\omega)[\eta]$, $2\left(\omega^2-\eta^2-2\omega\right)\in\mathbb{Q}(\eta)[\omega]$,
* $\omega^2-\eta^2\in\mathbb{Q}(\eta)[\omega]$,
* $\omega+1+\eta\in\mathbb{Q}(\omega)[\eta]$, $\omega+1-\eta\in\mathbb{Q}(\omega)[\eta]$,
* $\omega-1+\eta\in\mathbb{Q}(\omega)[\eta]$ et $\omega-1-\eta\in\mathbb{Q}(\omega)[\eta]$

sont non constants, sans facteur carré et deux à deux premiers entre eux. Par suite, aucun produit de la forme

$$\begin{array}{l}2^{n_1+n_2}\left(\omega^2-\eta^2+2\omega\right)^{n_1}\left(\omega^2-\eta^2-2\omega\right)^{n_2}\left(\omega^2-\eta^2\right)^{n_3}\\ \times\left(\omega+1+\eta\right)^{n_4}\left(\omega+1-\eta\right)^{n_5}\left(\omega-1+\eta\right)^{n_6}\left(\omega-1-\eta\right)^{n_7}\end{array}$$

avec $(n_i)_{i=1}^7\in\{0,1\}^7$ non nul n'est un carré dans $\mathbb{Q}(\omega)[\eta]$ (un tel produit est un polynôme non constant et sans facteur carré). Ainsi, aucun produit de la forme

$$\begin{array}{l}2^{n_1+n_2}\left(\omega^2-\eta^2+2\omega\right)^{n_1}\left(\omega^2-\eta^2-2\omega\right)^{n_2}\left(\omega^2-\eta^2\right)^{n_3}\\ \times\left(\omega+1+\eta\right)^{n_4}\left(\omega+1-\eta\right)^{n_5}\left(\omega-1+\eta\right)^{n_6}\left(\omega-1-\eta\right)^{n_7}\end{array}$$

(avec $(n_i)_{i=1}^7\in\{0,1\}^7$ non nul) n'est un carré dans $k=\mathbb{Q}(\eta,\omega,\rho)$.

Par ailleurs, les discriminants des polynômes (de degré 2)

$$b_1-1+\omega=\tfrac{1}{\omega^2-\eta^2}\rho^2-\left(\tfrac{\omega^2}{\omega^2-\eta^2}+\tfrac{\omega^2-\eta^2}{4}-\omega\right)\in\mathbb{Q}(\eta,\omega)[\rho],$$

$$b_1-1-\omega=\tfrac{1}{\omega^2-\eta^2}\rho^2-\left(\tfrac{\omega^2}{\omega^2-\eta^2}+\tfrac{\omega^2-\eta^2}{4}+\omega\right)\in\mathbb{Q}(\eta,\omega)[\rho],\text{ et}$$

$$2\left(2b_1-2+\omega^2-\eta^2\right)=\tfrac{4}{\omega^2-\eta^2}\rho^2-\left(\tfrac{4\omega^2}{\omega^2-\eta^2}-\left(\omega^2-\eta^2\right)\right)\in\mathbb{Q}(\eta,\omega)[\rho]$$

sont non nuls (car η et ω sont algébriquement indépendants), donc les polynômes $b_1-1+\omega\in\mathbb{Q}(\eta,\omega)[\rho]$, $b_1-1-\omega\in\mathbb{Q}(\eta,\omega)[\rho]$ et $2\left(2b_1-2+\omega^2-\eta^2\right)\in\mathbb{Q}(\eta,\omega)[\rho]$ sont non constants et sans facteur carré. Ces polynômes sont premiers entre eux car les éléments

$$2\omega=\left(b_1-1+\omega\right)-\left(b_1-1-\omega\right),$$

$$2\omega^2-2\eta^2-4\omega=2\left(2b_1-2+\omega^2-\eta^2\right)-4\left(b_1-1+\omega\right)$$

$$2\omega^2-2\eta^2+4\omega=2\left(2b_1-2+\omega^2-\eta^2\right)-4\left(b_1-1-\omega\right)$$

sont non nuls (η et ω sont algébriquement indépendants). Ainsi, aucun produit de la forme

$$2^{n_1}\alpha\left(2b_1-2+\omega^2-\eta^2\right)^{n_1}\left(b_1-1+\omega\right)^{n_2}\left(b_1-1-\omega\right)^{n_3}$$

(avec $\alpha\in\mathbb{Q}(\eta,\omega)^\times$ et (n_1,n_2,n_3) un triplet non nul d'éléments de $\{0,1\}$) n'est un carré dans $\mathbb{Q}(\eta,\omega)[\rho]$. Par suite, aucun produit de la forme

$$2^{n_1}\alpha\left(2b_1-2+\omega^2-\eta^2\right)^{n_1}\left(b_1-1+\omega\right)^{n_2}\left(b_1-1-\omega\right)^{n_3}$$

(avec $\alpha \in \mathbb{Q}(\eta,\omega)^\times$ et (n_1,n_2,n_3) un triplet non nul d'éléments de $\{0,1\}$) n'est un carré dans $k = \mathbb{Q}(\eta,\omega,\rho)$.

Nous remarquons que les polynômes

$$b_1 - \eta = \tfrac{1}{\omega^2-\eta^2}\rho^2 - \left(\tfrac{\eta^2}{\omega^2-\eta^2} + \tfrac{\omega^2-\eta^2}{4} + \eta\right) \in \mathbb{Q}(\eta,\omega)[\rho], \text{ et}$$

$$b_1 + \eta = \tfrac{1}{\omega^2-\eta^2}\rho^2 - \left(\tfrac{\eta^2}{\omega^2-\eta^2} + \tfrac{\omega^2-\eta^2}{4} - \eta\right) \in \mathbb{Q}(\eta,\omega)[\rho]$$

sont de degrés égaux à 2 et de discriminants non nuls. Par conséquent les polynômes $b_1 - \eta \in \mathbb{Q}(\eta,\omega)[\rho]$ et $b_1 + \eta \in \mathbb{Q}(\eta,\omega)[\rho]$ sont non constants et sans facteur carré. De plus, l'élément

$$2\eta = (b_1 + \eta) - (b_1 - \eta)$$

est non nul donc les polynômes $b_1 - \eta \in \mathbb{Q}(\eta,\omega)[\rho]$ et $b_1 + \eta \in \mathbb{Q}(\eta,\omega)[\rho]$ sont premiers entre eux. En particulier, le polynôme $b_1^2 - \eta^2$ est non constant et sans facteur carré. Le polynôme $b_1^2 - \eta^2$ n'est donc pas un carré dans $\mathbb{Q}(\eta,\omega)[\rho]$. Par suite, le polynôme $b_1^2 - \eta^2$ n'est pas un carré dans $k = \mathbb{Q}(\eta,\omega,\rho)$.

Le discriminant du polynôme

$$2b_1 + \omega^2 - \eta^2 - 1 = \frac{2}{\omega^2-\eta^2}\rho^2 - \left(\frac{2\eta^2}{\omega^2-\eta^2} - \frac{\omega^2-\eta^2}{2} + 1\right) \in \mathbb{Q}(\eta,\omega)[\rho]$$

est non nul. Le polynôme $2b_1 + \omega^2 - \eta^2 - 1$ est donc sans facteur carré. Ainsi, puisqu'il est non constant, le polynôme $2b_1 + \omega^2 - \eta^2 - 1$ n'est pas un carré dans $\mathbb{Q}(\eta,\omega)[\rho]$. Par suite, le polynôme $2b_1 + \omega^2 - \eta^2 - 1$ n'est pas un carré dans $k = \mathbb{Q}(\eta,\omega,\rho)$.

Les hypothèses du théorème 4.6.1 sont donc satisfaites. Par conséquent, le polynôme

$$P(x,y) := \left(y^2+1\right)\left(y^2 + C\left(x^2\right)\right)\left(y^4 + \left(1 + C\left(x^2\right)\right)y^2 + B\left(x^2\right)\right)$$

est positif ou nul sur $\mathbb{R}^2$, mais n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$. $\square$

Corollaire 4.6.3 *Soient $\eta := 23$ $\omega := 34$ et $\rho := 547$. Nous posons :*

$$b_1 = \tfrac{\rho^2-\eta^2}{\omega^2-\eta^2} + \tfrac{\eta^2-\omega^2}{4} = \tfrac{14063}{44},$$

$$B(x) := (x+b_1)^2 - \eta^2 = x^2 + \tfrac{14063}{22}x + \tfrac{196743825}{1936} \text{ et}$$

$$C(x) := 2(x+b_1) + \omega^2 - \eta^2 - 1 = 2x + \tfrac{27835}{22}.$$

Alors le polynôme

$$P(x,y) := \left(y^2+1\right)\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right) \in \mathbb{Q}(x,y)$$

est positif ou nul sur $\mathbb{R}^2$*, mais n'est pas une somme de trois carrés dans* $\mathbb{R}(x,y)$*.*

Démonstration.

Nous vérifions les hypothèses du théorème 4.6.1 lorsque $\eta = 23$, $\omega = 34$ et $\rho = 547$.

Tout d'abord nous remarquons que les éléments

* $\eta = 23,$ et $\rho = 547,$

* $\omega^2 - \eta^2 - 2 - 2\eta = 579$ et $\omega^2 - \eta^2 - 2 + 2\eta = 671,$

* $\left(\omega^2 - \eta^2 - 2\right)^2 - 4\eta^2 - 4 = 388505,$

* $\omega^2 - \eta^2 - 1 + 2\eta = 672$ et $\omega^2 - \eta^2 - 1 - 2\eta = 580,$

* $\left(\omega^2 - \eta^2 - 1\right)^2 - 4\eta^2 - 1 = 389759,$

* $\omega^2 - \eta^2 - 2\eta = 581$ et $\omega^2 - \eta^2 + 2\eta = 673$

sont non nuls. Nous avons aussi les inégalité

* $\omega = 34 > 24 = 1 + |\eta|,$

* $\omega^2 - 2\omega = 1088 > 529 = \eta^2$ et

* $b_1 - 1 - \frac{\omega^2-\eta^2}{2} = \frac{225}{44} > 0.$

De plus, les nombres rationnels

a. $(\omega^2-\eta^2-2\omega)(\omega^2-\eta^2+2\omega)=388505=5\times13\times43\times139$,

b. $(2b_1-2+\omega^2-\eta^2)(\omega^2-\eta^2-2\omega)=\frac{15547467}{22}=\frac{3\times13\times43\times73\times127}{2\times11}$,

c. $(2b_1-2+\omega^2-\eta^2)(\omega^2-\eta^2+2\omega)=\frac{19330035}{22}=\frac{3\times5\times73\times127\times139}{2\times11}$,

d. $2\left(\omega^2-\eta^2-2\omega\right)(b_1-1-\omega)=\frac{7000357}{22}=\frac{7\times13\times43\times1789}{2\times11}$,

e. $2\left(\omega^2-\eta^2+2\omega\right)(b_1-1+\omega)=\frac{10782925}{22}=\frac{5^2\times29\times107\times139}{2\times11}$,

f. $2\left(2b_1-2+\omega^2-\eta^2\right)(b_1-1+\omega)=\frac{431518695}{484}=\frac{3\times5\times29\times73\times107\times127}{2^2\times11^2}$,

g. $2\left(2b_1-2+\omega^2-\eta^2\right)(b_1-1-\omega)=\frac{348302199}{484}=\frac{3\times7\times73\times127\times1789}{2^2\times11^2}$,

h. $$\begin{aligned}\left((b_1-1)^2-\omega^2\right)\left(\left(\omega^2-\eta^2\right)^2-4\omega^2\right) &= \frac{75484324504225}{1936}\\ &= \frac{5^2\times7\times13\times29\times43\times107\times139\times1789}{2^4\times11^2},\end{aligned}$$

l. $2\left(\omega^2-\eta^2\right)\left(2b_1-2+\omega^2-\eta^2\right)=1585341=3^2\times19\times73\times127$,

o. $b_1^2-\eta^2=\frac{196743825}{1936}=\frac{3^2\times5^2\times31\times67\times421}{2^4\times11^2}$, et

p. $2b_1+\omega^2-\eta^2-1=\frac{27835}{22}=\frac{5\times19\times293}{2\times11}$

ne sont pas des carrés dans $\mathbb{Q}$ (ils sont tous de valuation impaire en au moins un élément premier de $\mathbb{Z}$).

Nous devons maintenant vérifier les conditions g, h, i, k et l.

i. et j. La valuation en 19 de $\omega^2-\eta^2=3\times11\times19$ est 1. Or les valuations en 19 des nombres rationnels

$$\omega^2-\eta^2-2\omega=559=13\times43,$$

$$\omega^2-\eta^2+2\omega=695=5\times139,$$

$$(\omega+1)^2-\eta^2=696=2^3\times3\times29 \text{ et}$$

$$(\omega-1)^2-\eta^2=560=2^4\times5\times7$$

sont nulles, donc les éléments de la forme

$$2\left(\omega^2-\eta^2\right)\left(\omega^2-\eta^2-2\omega\right)\left(\left(\omega+1\right)^2-\eta^2\right)^n \text{ ou}$$

$$2\left(\omega^2-\eta^2\right)\left(\omega^2-\eta^2+2\omega\right)\left(\left(\omega-1\right)^2-\eta^2\right)^n$$

(avec $n\in\{0,1\}$) ne sont pas des carrés dans $\mathbb{Q}$ (leurs valuations en 19 sont égales à 1).

k. Supposons qu'il existe un triplet $(n_{1,2}\,,n_3)$ non nul d'éléments de $\{0,1\}$ tel que

$$\left(\left(b_1-1\right)^2-\omega^2\right)^{n_1}\left(\left(\omega-1\right)^2-\eta^2\right)^{n_2}\left(\left(\omega+1\right)^2-\eta^2\right)^{n_3}$$

soit un carré dans $\mathbb{Q}$.

La valuation en 107 de

$$\left(b_1-1\right)^2-\omega^2=\frac{194294345}{1936}=\frac{5\times7\times29\times107\times1789}{2^4\times11^2}$$

est 1. Or les valuations en 107 des nombres rationnels

$$\left(\omega+1\right)^2-\eta^2=696=2^3\times3\times29 \text{ et}$$

$$\left(\omega-1\right)^2-\eta^2=560=2^4\times5\times7$$

sont nulles, donc $n_1=0$. De même, la valuation en 3 de

$$\left(\omega+1\right)^2-\eta^2=696=2^3\times3\times29$$

est 1 et les valuations en 3 des nombres rationnels

$$\left(b_1-1\right)^2-\omega^2=\tfrac{194294345}{1936}=\tfrac{5\times7\times29\times107\times1789}{2^4\times11^2} \text{ et}$$

$$\left(\omega-1\right)^2-\eta^2=560=2^4\times5\times7$$

sont nulles donc $n_3=0$. Nous aboutissons à une contradiction : comme le triplet (n_1,n_2,n_3) n'est pas nul, le nombre rationnel

$$\left(\omega-1\right)^2-\eta^2=560=2^4\times5\times7$$

doit être un carré dans de $\mathbb{Q}$ (alors que sa valuation en 7 est 1). Nous en déduisons qu'il n'existe aucun triplet $(n_{1,2}\,,n_3)$ non nul d'éléments de $\{0,1\}$ tel que

$$\left(\left(b_1-1\right)^2-\omega^2\right)^{n_1}\left(\left(\omega-1\right)^2-\eta^2\right)^{n_2}\left(\left(\omega+1\right)^2-\eta^2\right)^{n_3}$$

soit un carré dans $\mathbb{Q}$.

m. La valuation en 139 du nombre rationnel

$$\left(\omega^2 - \eta^2 + 2\omega\right) = 695 = 5 \times 139$$

est 1. or les valuations en 139 des nombres rationnels

$$(b_1 - 1 + \omega) = \tfrac{15515}{44} = \tfrac{5\times 29\times 107}{2^2\times 11}$$

$$2(\omega^2 - \eta^2) = 1254 = 2 \times 3 \times 11 \times 19,$$

$$2b_1 - 2 + \omega^2 - \eta^2 = \tfrac{27813}{22} = \tfrac{3\times 73\times 127}{2\times 11},$$

$$\omega - 1 - \eta = 10 = 2 \times 5 \text{ et}$$

$$\omega - 1 + \eta = 56 = 2^3 \times 7$$

sont nulles, donc les éléments de la forme

$$2^{n_1}\left(\omega^2 - \eta^2 + 2\omega\right)(b_1 - 1 + \omega)\left(\omega^2 - \eta^2\right)^{n_1}\left(2b_1 - 2 + \omega^2 - \eta^2\right)^{1-n_1} \times (\omega - 1 - \eta)^{1-n_2}(\omega - 1 + \eta)^{n_2}$$

(avec n_1, $n_2 \in \mathbb{N}$) ne sont pas des carrés dans $\mathbb{Q}$ (leurs valuations en 139 sont égales à 1).

n. La valuation en 139 du nombre rationnel

$$\left(\omega^2 - \eta^2 + 2\omega\right) = 695 = 5 \times 139$$

est 1. or les valuations en 139 des nombres rationnels

$$2(\omega^2 - \eta^2) = 1254 = 2 \times 3 \times 11 \times 19,$$

$$2b_1 - 2 + \omega^2 - \eta^2 = \tfrac{27813}{22} = \tfrac{3\times 73\times 127}{2\times 11},$$

$$\omega - 1 - \eta = 10 = 2 \times 5 \text{ et}$$

$$\omega - 1 + \eta = 56 = 2^3 \times 7$$

sont nulles, donc les éléments de la forme

$$2^{1-n_1}\left(\omega^2 - \eta^2 + 2\omega\right)\left(\omega^2 - \eta^2\right)^{n_1}\left(2b_1 - 2 + \omega^2 - \eta^2\right)^{n_1} \times (\omega - 1 - \eta)^{1-n_2}(\omega - 1 + \eta)^{n_2},$$

(avec n_1, $n_2 \in \mathbb{N}$) ne sont pas des carrés dans $\mathbb{Q}$ (leurs valuations en 139 sont égales à 1).

Les hypothèses de la proposition 4.6.1 sont donc vérifiées. D'après cette proposition, le polynôme

$$P(x,y) := \left(y^2+1\right)\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right) \in \mathbb{Q}(x,y)$$

est positif ou nul sur $\mathbb{R}^2$, mais n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$. $\square$

Bibliographie

[Art27] E. Artin. über die zerlegung definiter funktionen in quadrate. Hamb. Abh, 5 :100–115, 1927.

[BCR98] J. Bochnak, M. Coste, and M.-F. Roy. Real algebraic geometry, volume 36 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1998. Translated from the 1987 French original, Revised by the authors.

[BM88] J.-B. Bost and J.-F. Mestre. Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. Gaz. Math., (38) :36–64, 1988.

[CEP71] J. W. S. Cassels, W. J. Ellison, and A. Pfister. On sums of squares and on elliptic curves over function fields. J. Number Theory, 3 :125–149, 1971.

[CF96] J. W. S. Cassels and E. V. Flynn. Prolegomena to a middlebrow arithmetic of curves of genus 2, volume 230 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1996.

[Chr76] M. R. Christie. Positive definite rational functions of two variables which are not the sum of three squares. J. Number Theory, 8(2) :224–232, 1976.

[CT93] J.-L. Colliot-Thélène. The Noether-Lefschetz theorem and sums of 4-squares in the rational function field $\mathbf{R}(x, y)$. Compositio Math., 86(2) :235–243, 1993.

[Gau00] P. Gaudry. Algorithmique des courbes hyperelliptiques et applications à la cryptologie. PhD thesis, 2000.

[Har82] J. Harris. Theta-characteristics on algebraic curves. Trans. Amer. Math. Soc., 271(2) :611–638, 1982.

[Hil88] D. Hilbert. über die darstellung definiter formen als summen von formen-quadraten. Math. Ann, 32 :342–350, 1888.

[HM01] J. Huisman and L. Mahé. Geometrical aspects of the level of curves. J. Algebra, 239(2) :647–674, 2001.

[HS00] M. Hindry and J. H. Silverman. Diophantine geometry, volume 201 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2000. An introduction.

[Igu60] J. Igusa. Arithmetic variety of moduli for genus two. Ann. of Math. (2), 72 :612–649, 1960.

[Kna92] A. W. Knapp. Elliptic curves, volume 40 of Mathematical Notes. Princeton University Press, Princeton, NJ, 1992.

[Lam73] T. Y. Lam. The algebraic theory of quadratic forms. W. A. Benjamin, Inc., Reading, Mass., 1973. Mathematics Lecture Note Series.

[Lan97] S. Lang. Survey of Diophantine Geometry. Springer, 1997.

[Mac00] O. Macé. Sommes de trois carrés en deux variables et représentation de bas degré pour le niveau des courbes réelles. PhD thesis, Université de Rennes 1, 2000.

[Mah90] L. Mahé. Level and Pythagoras number of some geometric rings. Math. Z., 204(4) :615–629, 1990.

[Mah92] L. Mahé. "Level and Pythagoras number of some geometric rings" [Math. Z. **204** (1990), no. 4, 615–629 ; MR1062139 (91g :11034)] and erratum. Math. Z., 209(3) :481–483, 1992.

[MM05] O. Macé and L. Mahé. Sommes de trois carrés de fractions en deux variables. Manuscripta Math., 116(4) :421–447, 2005.

[Mum84] D. Mumford. Tata lectures on theta. II, volume 43 of Progress in Mathematics. Birkhäuser Boston Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[OU73] F. Oort and K. Ueno. Principally polarized abelian varieties of dimension two or three are Jacobian varieties. J. Fac. Sci. Univ. Tokyo Sect. IA Math., 20 :377–381, 1973.

[Pfi67] A. Pfister. Zur Darstellung definiter Funktionen als Summe von Quadraten. Invent. Math., 4 :229–237, 1967.

[Sch95] E. F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. J. Number Theory, 51(2) :219–232, 1995.

[Sch98] E. F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. Math. Ann., 310(3) :447–471, 1998.

[Ser68] J.-P. Serre. Corps locaux. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Ser84] J.-P. Serre. Groupes algébriques et corps de classes. Publications de l'Institut Mathématique de l'Université de Nancago [Publications of the Mathematical Institute of the University of Nancago],

7. Hermann, Paris, second edition, 1984. Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics], 1264.

[Sil92] J. H. Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[Sil94] J. H. Silverman. Advanced topics in the arithmetic of elliptic curves, volume 151 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1994.

[ST92] J. H. Silverman and J. Tate. Rational points on elliptic curves. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[Sti93] H. Stichtenoth. Algebraic function fields and codes. Universitext. Springer-Verlag, Berlin, 1993.

[Sto01] M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. Acta Arith., 98(3) :245–277, 2001.

[ZS58] O. Zariski and P. Samuel. Commutative algebra, Volume I. The University Series in Higher Mathematics. D. Van Nostrand Company, Inc., Princeton, New Jersey, 1958. With the cooperation of I. S. Cohen.